DOC. 000233

CPL/AC

PREGÃO 050/2003

LOCAÇÃO DE EQUIPAMENTOS DE INFORMÁTICA INCLUINDO ASSISTÊNCIA TÉCNICA E TREINAMENTO

HP INVENT – MANUAL APÊNDICES AA A AR

2003
PASTA 05

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0001
Fls:
3701
Doc:

Apêndice AA

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 0002
Doc: 3701

ECT 3.176 L. CPMI-K

MODELS

HP Ultrium 400 GB Data Cartridge

C7972A, Worldwide

Feature List:

- 200 GB native capacity at 2:1 compression
- Unique red cartridge shell to assist with identification in mixed media vaults
- Superior 'smart grabber' mechanism and mechanical interlock to prevent the leader pin from being pulled inside the tape housing (a key weakness of DLT media). Sensors detect proper connection and prevent leader loss that would ruin the tape.
- Simplified tape path to reduce wear and tear.
- Lowest media cost per GB at launch of *any* tape technology.
- LTO cartridge memory in media to improve access time and provide enhanced media monitoring.
- Improved cartridge robustness and durability

OVERVIEW

Backed by HP's exhaustive media qualification process, the C7972A HP Ultrium 400GB data cartridge supports the launch of the HP StorageWorks Ultrium 460 Tape Drive. Building on the class-leadership of the Linear Tape Open standard, HP Ultrium 2 cartridges provide exceptional reliability with best-in-class high performance; the new format minimizes network interruption by being capable of protecting nearly 216 GB/hour of data (88% faster than SDLT 320) and storing up to 400GB on one piece of media (double the capacity of Ultrium 1 tapes).

Customer Benefits Include:

- high-capacity: supports capacities up to 400 GB
- high-performance: with HP StorageWorks Ultrium 460 tape drive delivers up to 60 MB/sec compressed transfer rate
- reliable: combines the best of proven technologies to offer users improvements in capacity and performance.
- open standard: for use in all HP and non-HP LTO Ultrium 2 products
- easy to use: possesses a distinctive red cartridge shell

KEY FEATURES

- Tested to extremes in HP's media laboratory, to a level of specification unique to Hewlett-Packard. Many of the test procedures required for HP Brand qualification (e.g. load/unload, shoeshine, drop testing and thermal aging) are not required for the Ultrium logo.
- 200 GB (native), 400 GB (2:1)
- Supports transfer speeds of 30 MB/s (native), 60 MB/s (2:1)
- Unique red cartridge shell
- Compatible with all HP and non-HP LTO Ultrium tape products
- LTO Cartridge Memory
- Superior mechanism, tape path and tape engagement
- Durable cartridge designed to minimize wear and debris (important in automation)

PRODUCT HIGHLIGHTS

'ium 2 Tape Technology

Ultrium 2 tape drive technology uses a linear format of 512 tracks, writing eight (8) tracks simultaneously. The data is written in a serpentine pattern; the tape reverses direction after each set of eight tracks is written.

Ultrium formats are open standards. This means that data written on any HP StorageWorks Ultrium 460 tape drive for ProLiants can be interchanged directly with Ultrium 2 tape drives from other vendors.

RQS Nº 03/2005 - CN - CPMI - CORREIOS
0003
Fls:
3701
Doc:

PRODUCT HIGHLIGHTS *(continued)*

High Reliability

HP ensures the highest level of quality with media specifications that far exceed industry standards.

- HP has 20 custom-built testing chambers that are in use 24 hours per day, 365 days per year.
- It is doubtful if any other media supplier carries out such exhaustive qualification of the drive and media as they are used in the field. This is because no media supplier is exposed to support of hardware in the field and has a vested interest in reducing media-induced hardware issues.
- In 2001, 170,000 different media tests were performed, accounting for 1.3 million test hours.
- HP testing includes procedures like drop testing, load/unload, environmental stress tests and archival simulation that are not required to gain the Ultrium logo.

LTO Ultrium 100/200 GB tape technology uses a "best of breed" technology approach, taking the best features from other tape technologies and combining them into a single new technology without the need for design compromises to accommodate legacy compatibility requirements. Designed for the demanding environment of large-scale libraries, Ultrium 400 GB media is certified for 1 million passes or 100 full back ups and has a 30 year archival storage life.

Compression

LTO-DC is an enhanced version of Advanced Lossless Data Compression (ALDC) hardware compression. Compression is automatically turned "off" if the compressed data would cause an overall expansion in data size.

Compatibility Testing

HP Ultrium 400 GB data cartridges are fully supported and compatible with HP StorageWorks Ultrium tape products. Because HP Ultrium media is Ultrium 2 logo compliant, it may be used with any other non-HP device that bears the Ultrium 2 logo.

Backward Read Compatible

HP Ultrium 400 GB media cannot be read or used to write new data in an Ultrium 1 drive or automation product.

HP Branded Media Specification

HP believes that its test program for HP Ultrium media is the most thorough and comprehensive in the industry. In order to carry the HP Brand, designated cartridges must satisfy an exhaustive battery of additional procedures that relate directly to how the product is used in real life situations when real data and real businesses are at stake. Some of these procedures – e.g. "five corner" environmental interchange, load/unload for automation, ageing simulation and drop testing are not found in the standard logo test. Over 1 million test hours on media and drives per year ensures that HP Ultrium media will always offer maximum reliability even in the most extreme conditions.

Why Buy LTO?

If you have not yet standardized on a large-tape format then LTO Ultrium tape technology is the preferred choice offering

- Highest reliability through no compromise design and innovative features like Data Rate Matching.
- High capacity to meet the challenges of data deluge
- High performance - even on slower hosts
- An industry standard - Linear Tape Open format
- Investment protection - with a four generation roadmap with plans to deliver an 800 GB (native) tape drive by the year 2006

Service and Support

Includes a limited lifetime warranty, fully supported by a worldwide network of resellers and service providers and toll-free 7 x 24 technical phone support during the warranty period.

Warranty

Limited lifetime warranty.

ECT 3.174 2 CPI - AC

SPECIFICATIONS

Dimensions (H x W x D)	**Shipping**	
	HP Ultrium 400 GB Data Cartridge (single pack)	1.8 x 4.45 x 4.37 in/2.1 x 11.3 x 11.1 cm
Weight	**Shipping**	
	HP Ultrium 400 GB Data Cartridge (single pack)	0.63 lb/285.2 g
UPC Code	HP Ultrium 400 GB Data Cartridge (single pack)	8 08736-39584 7
Capacity	200 GB native/400 GB compressed (2:1)	
	512 tracks with a track pitch of 20.17 um	
Tape Format	Recording Method	Linear 1/2" tape, 8 track parallel recording.
	Recording Format	Ultrium Generation 2
Media Type	Ultrium 2 media – 609m, 1/2" tape, Metal Particle (MP++) formulation with 4K Cartridge Memory	
Media Durability	1,000,000 passes on any area of tape, equates to over 20,000 end-to-end passes/100 full tape backups	
Basefilm Type	6 um Metal particle PEN	
e Thickness	8.9um ± 0.3um	
Magnetic Layer Coercivity	2,350 Oe	
Tape Life	30 years archival storage	
Environmental Details	Operating Temperature	50 to 113 ° F/10 to 45 ° C
(Media should not be used outside of these parameters)	Day to Day Storage Temperature	60 to 90 ° F/16 to 32 ° C
	Long Term Storage Temperature – Ambient	41 to 73 ° F/5 to 23 ° C
	Maximum Wet Bulb Temperature	79 ° F/26 ° C
	Non Condensing Relative Humidity	10 to 80%

CONFIGURATION INFORMATION

RELATED OPTIONS

Media	HP Ultrium 400 GB* data cartridge ** (recommended)	C7972A
	HP Ultrium 200 GB* data cartridge** (*assumes 2:1 compression ratio)	C7971A
	HP Ultrium Universal cleaning cartridge**	C7978A

** Customers and partners can order additional LTO media (part no.: C7971A and C7972A) and LTO cleaning cartridges (part no.: C7978A) as HP third-party products through traditional Major Account Direct, Partner Direct, and Compaq Direct processes. This is the same method that HP printers are ordered via Compaq direct systems today.

© 2002 Hewlett-Packard Company

Hewlett-Packard, the Hewlett-Packard logo, and StorageWorks are trademarks of Hewlett-Packard Company in the U.S. and/or other countries. All other product names mentioned herein may be trademarks of their respective companies.

Hewlett-Packard shall not be liable for technical or editorial errors or omissions contained herein. The information is provided "as is" without warranty of any kind and is subject to change without notice. The warranties for Hewlett-Packard products are set forth in the express limited warranty statements accompanying such products. Nothing herein should be construed as constituting an additional warranty.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0004
Fls:
Doc:

Apêndice AB

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 0005
Doc: 3701

E C T
3.173
1
CPI - AS

User Guide

rp5400 Family of Servers

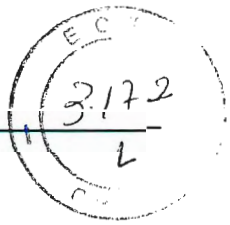
First Edition

Manufacturing Part Number : A5191-96018
November 2002

USA

© Copyright 2002

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 0006
Doc: 3701



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.

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.

Copyright Notices. ©copyright 1983-2002 Hewlett-Packard Company, all rights reserved.

Windows", Windows NT", Windows 95", Windows 2000", and Windows XP" are registered trademarks of Microsoft in the U.S. and other countries.

Reproduction, adaptation, or translation of this document without prior written permission is prohibited, except as allowed under the copyright laws.

Contents

ECT 3.171 2 CPI-AC

1. Server Overview

2. Server Unpacking and Installation

Factory Integrated rp54xx Cabinet Installation 4
Receive and Unpack A Non-Integrated Server 7
Unpacking the server 7
Install Deskside Server 10
Install Stand-Alone Server in a Cabinet. 13
Stationary L-Bracket Rail Assembly 19
Identifying Approved Non-E-Series HP Cabinets. 19
Identifying E-Series HP Cabinets 20
Identifying Static Rail Kit 20
Installing Stationary Rails. 21

3. Installing Additional Components

Additional Components 24
Installing Memory 25
Memory Configuration Rules. 25
Installing Peripheral Component Interconnect (PCI) Cards. 30
rp5400/rp5450 PCI Card Slots. 30
rp5470 PCI Card Slots 31
PCI I/O Card Installation Restrictions 32
PCI I/O Card Installation Order 32
Installing a PCI Card 34
Online Addition/Replacement (OLA/R) of PCI I/O cards 36
Installing Graphics 37
Graphics Troubleshooting 43
Installing Disk Drives 44

4. Cable Connections

Core I/O Connections. 48
Revision A GSP. 48
Revision B GSP. 49
Guardian Service Processor (GSP) Overview. 51
GSP LAN. 51
GSP RS-232. 51
GSP Features 51
Revision A GSP. 52
Revision B GSP. 52
Configure System Consoles 53
GSP Cables 54
Configure RS-232 Console 54
Configure Remote Console 58
Configure the LAN Console 59
Configure the Web Console 61
Secure Web Console Installation. 66

ROS Nº 03/2005 - CN
CRMI - CORREIOS
Fls: 0007
3701
Doc:

Contents

GSP Configurable Parameters 69
Adding Users 69
Removing Users 70
Return the GSP to Default Configurations 71
rp54xx Server Boot Process 72
Initial Power-up 74

5. Utilities

Configuring the Rev A Guardian Service Processor (GSP) 78
Configuring the GSP LAN Port 78
Adding Users 78
Removing Users 80
Changing the Default GSP Configuration 80
Configuring the Rev B Guardian Service Processor (GSP) 81
Configuring the GSP LAN Port 81
Adding Users 81
Removing Users 83
Changing the Default GSP Configuration 83

6. Troubleshooting

Determine Current System State 86
Troubleshooting and FRU identification 87
Problem Symptoms and Repair Actions 87
Chassis Code to FRU Decode 91
Cross-Referencing Chassis Log Errors to rp54xx FRUs 91
Interpreting System Alerts 94
Interpreting Service Processor Error Chassis Logs 96
Interpreting Chassis Logs Using the chassis_code.codes File 98
rp5400 and rp5450 System Block Diagram 100
rp5400 and rp5450 I/O Block Diagram 101
rp5430 and rp5470 System Block Diagram 102
rp5430 and rp5470 I/O Block Diagram 103
Run/Attention/Fault LED States 104
PCI I/O LED States 112
Expansion I/O LED States 114
GSP LED States 116
LAN/SCSI LED States 118
Fan, Power Supply, and Disk LED States 119

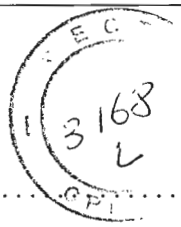
7. Removing and Replacing Components

List of Changeable Parts with Remove and Replace Components 122
Cardcage Fan 122
Core I/O 122
HotSwap Chassis Fan 122
Disk Drive 123
Display Board 123

Front Bezel 123
Memory DIMM 123
PCI I/O Card 124
Power Supply 124
HotSwap Power Converter Fan 124
Platform Monitor 124
Processor Support Module 125
Individual Component Remove/Replace Instructions 126
Extend the Server out the Front 126
Insert the Server from the Front 127
Stand-alone Server Cover Removal 128
Stand-alone Server Cover Replacement 130
Top Cover Removal 131
Top Cover Replacement 132
Side Cover Removal 133
Side Cover Replacement 134
Front Bezel Removal (Single Piece) 135
Front Bezel Replacement (Single Piece) 136
Front Bezel Removal (Two Piece) 137
Front Bezel Replacement (Two Piece) 138
Core I/O Removal 139
Core I/O Replacement 140
PCI Card Separator/Extractor Removal 142
PCI Card Separator/Extractor Replacement 143
HotPlug Disk Drive Removal 144
HotPlug Disk Drive Replacement 149
HotSwap Chassis Fan Cover Removal 152
HotSwap Chassis Fan Cover Replacement 153
HotSwap Chassis Fan Removal 154
HotSwap Chassis Fan Replacement 155
HotSwap Card Cage Fan Removal 156
HotSwap Card Cage Fan Replacement 157
HotSwap Power Supply Removal 158
HotSwap Power Supply Replacement 159
HotSwap Power Converter Fan Removal 160
HotSwap Power Converter Fan Replacement 161
Processor Support Module Removal 162
Processor Support Module Replacement 163
Memory DIMM Removal 164
Memory DIMM Replacement 165
Display Board Removal 166
Display Board Replacement 167
Platform Monitor Removal 168
Platform Monitor Replacement 170
PCI I/O Card Removal 172
PCI I/O Card Replacement 173

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 0008
Doc: 3701

Contents



A. Parts and Accessories

CRU Physical Location 176
Customer Replaceable Unit Part Numbers 179

B. System Specifications

Dimensions 182
Uncrating Space 182
Space Requirements 182
Computer Room Physical Space Requirements 183
Computer Room Unpacking Space 184
Electrical 185
Office High Availability Requirements 185
Power Protection 185
Modular PDUs 186
System Power Requirements 186
LAN and Telephone 187
Acoustic Safety Standards 188
Altitude Operation Standards 189
Effects of Altitude 189
Temperature and Humidity Operating Standards 190
Thermal Protection Features 190

C. General Site Preparation Guidelines

Electrical Factors 192
Computer Room Safety 192
Power Consumption 193
Electrical Load Requirements (Circuit Breaker Sizing) 193
Power Quality 193
Distribution Hardware 194
Grounding Systems 195
System Installation Guidelines 197
Environmental Elements 198
Computer Room Preparation 198
Cooling Requirements 198
Humidity Level 200
Dust and Pollution Control 200
Metallic Particulate Contamination 201
Electrostatic Discharge (ESD) Prevention 202
Acoustics 202
Facility Characteristics 203
Floor Loading 203
Windows 205
Space Requirements 206
Delivery Space Requirements 206
Operational Space Requirements 206
Floor Plan Grid 206

Typical Installation Schedule 207
Site Inspection 208
Delivery Survey 212

E.C.T.
3.167
L
CPI - K

ROS Nº 03/2005 - CN
CPMI - CORREIOS
0009
Fls:
3791
Doc:

ECT 3.166 2

Table 6-1. Problem Symptoms and Repair Actions 87
Table 6-2. Chassis Log Error to FRU Decoder 91
Table A-1. Exchange CRUs 179
Table A-2. Non-Exchange CRUs 180
Table B-1. Power Requirements 186
Table C-1. Effect of Humidity on ESD Charge Levels 202
Table C-2. Floor Loading Term Definitions 203
Table C-3. Typical Raised Floor Specifications 204
Table C-4. Customer and Hewlett-Packard Information 208
Table C-5. Site Inspection Checklist 209

RQS Nº 03/2005 - CN
CRMI - CORREIOS
0010
Fls:
Doc: 3701

E C T
3.165
2
CPI - AC

Figure A-1. Server Rear View 176
Figure A-2. Side Service Bay 177
Figure A-3. System Board (Access via Top Service Bay) 177
Figure A-4. Server Front 178
Figure C-1. Raised Floor Metal Strip Ground System 196
Figure C-2. Delivery Survey (Part 1) 213
Figure C-3. Delivery Survey (Part 2) 214

RQS Nº 03/2005 - C.N
CPMI - CORREIOS
0011
Fls:
7701
Doc:

3.164
2

Preface

Printing History

The Printing History below identifies the edition dates of this manual. Updates are made to this publication on an unscheduled, *as needed*, basis. The updates will consist of a complete replacement manual and pertinent on-line or CD-ROM documentation.

First Edition ..... November 2002

What's New?

The, *Upgrade Guide, rp5400 Family of Servers*, is new and was developed to provide customers with system maintenance information for those components called customer replaceable units (CRUs). Maintenance of CRUs does not require HP customer engineering services, except when specifically cautioned. The cautions are shown primarily to protect customer product warrantees.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0012
Fls:
Doc: 2791

3.163
2

1 Server Overview

The rp5400 family of servers are 1-way to 4-way servers based on the PA-RISC processor architecture. The rp5400 family of servers accommodate up to 16GB of memory and internal peripherals including disks and DVD ROM/Tape. High availability features include HotSwap fans and power supplies, and HotPlug internal disk drives. The supported operating system is HP-UX.

RGS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 0013
Doc: 3791

3.162
2
CPI - AA

2 Server Unpacking and Installation

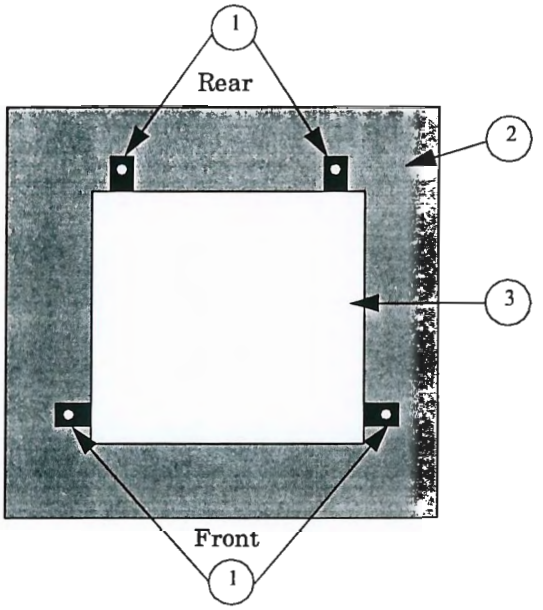
RQS Nº 03/2005 - CN
CPMI - CORREIOS
0014
Fls:
3701
Doc:

3.161

Factory Integrated rp54xx Cabinet Installation

A factory integrated server is one in which the rp54xx server and associated components are pre-assembled and shipped from the factory already installed in a Hewlett-Packard E-Series cabinet. Factory integrated systems reduce the amount of time required to set-up and begin server operation.

1. Carefully remove the carton and anti-static bag from the pallet.
2. Remove the front two (2) L-brackets. Retain the 1/2-inch bolts for later use.



1. Shipping L-Bracket
2. Shipping Pallet
3. Cabinet (Top View)

NOTE As viewed from the front, one bracket is located on each side at the base of the cabinet near the front.

ECT 3.160 2 CPI-AC

3. At the rear of the cabinet:
   a. Open the door.
   b. Remove the anti-tip foot by removing and retaining the two (2) 1/2-inch bolts.

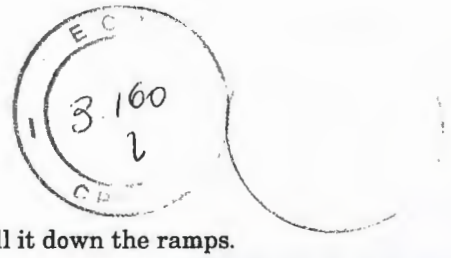
For Shipping: L-brackets are mounted behind anti-tip foot. Same bolts secure both.

   c. Remove the two (2) L-brackets (revealed by removing the anti-tip foot).
4. Remove the two ramps from the pallet and carefully place them into the slots at the front of the pallet.

WARNING **Use extreme care when rolling the racked system down the ramps. A rack containing one rp54xx can weigh up to 418 lbs. Do not stand in front of the ramps when rolling the cabinet off the pallet or injury may occur. All but the smallest configurations require two persons to safely remove the rack from the pallet.**

If anti-tip feet or ballast are not installed or are improperly installed the cabinet can tip. Failure to follow this precaution can cause injury to personnel or damage to equipment.

RGS Nº 03/2005 - CN
CPMI - CORREIOS
0015
Fls:
Doc: 701



5. Straighten the rollers on the cabinet base, if needed, and carefully roll it down the ramps.

WARNING ***After removing the server from the pallet, Do not move the cabinet unless the anti-tip feet are installed!*** **The cabinet can tip if care is not used. Due to their low ground clearance the feet may catch on irregularities on the floor, thresholds, or ramps.**

Do not move the cabinet without first installing the anti-tip feet. **The cabinet may tip if moved without the anti-tip feet or ballast installed.**

Do not move the cabinet after installing the anti-tip feet unless they are in the fully-raised position. **Once installed, the anti-tip feet must be fully raised to allow ground clearance.**

Because of their low ground clearance, the fully-raised anti-tip feet may need to be removed *temporarily* to clear some obstacles such as door jambs, ramps, and other large irregularities or obstructions on the floor.

If you must temporarily remove the anti-tip feet to clear an obstacle, use extreme caution when moving the cabinet. Always reinstall the anti-tip feet as soon as the obstacle has been cleared.

Lower and secure both the anti-tip feet and the cabinet leveling/stabilizer feet once the cabinet is in place.

Failure to follow these precautions can result in equipment damage or personal injury.

---

6. Install the front and rear anti-tip feet using the 1/2 inch bolts provided. Ensure that the anti-tip feet are installed in the fully up position in the mounting slots. This will provide maximum ground clearance while moving the cabinet to its final position.
7. Carefully move the cabinet to its installation location.
8. Lower the anti-tip feet to the fully down position and adjust the cabinet leveling feet for best cabinet stability.

ECT
3.159
L

Receive and Unpack A Non-Integrated Server

WARNING **The typical rp54xx system can weigh up to 68kg (150lbs). *HP recommends using an an approved lifting device.* Lift and move the server in accordance with all local safety regulations. Failure to follow this precaution can cause injury to personnel or damage to equipment.**

Unpacking the server

The following procedure describes the steps involved in unpacking the server, whether to function as a stand-alone Deskside unit, or to be integrated into a cabinet.

Step 1. Remove the shipping carton and anti-static bag from the server as depicted below.

ROS Nº 03/2003 - CN
CPMI - CORREIOS
0016
Fls:
Doc:

3.158
L

NOTE The packaging for rp74xx and rp54xx servers is the same, rp74xx is shown.

Step 2. If you are moving the server manually, use three people to lift the server from the packing material and pallet. Carefully move the server to the selected location.

Step 3. If you are moving the server by an approved lifting device (such as Genie Lift ™), remove the tear flap from the front lip of the carton bottom to allow access to the server, as illustrated below. Removal of the tear flap will reveal a slot between the bottom of the server and the inside bottom of the cardboard box.

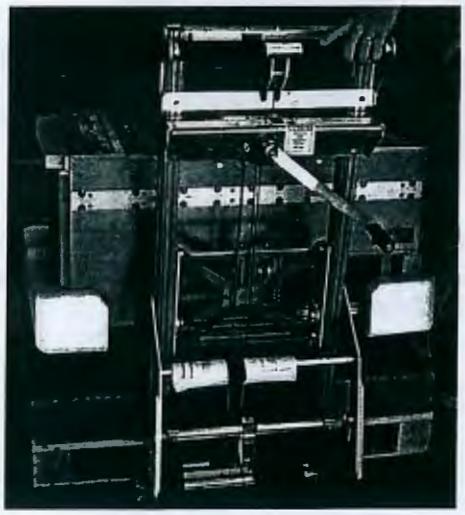
3.157
2

Step 4. Carefully raise the lift's platform so that it will slide into the slot located ***under*** the center of the server, but ***over*** the top of the pallet.

Lifting Device Platform.

NOTE The server's center of gravity will vary with the hardware configuration, but it is generally located slightly behind the middle of the server.

Step 5. Raise the lifting device platform enough for the server to clear the pallet and packing materials, as show below.



RQS Nº 03/2005 - CN
CPMI - CORREIOS
0017
Fls:
3701
Doc:

3.156
2

Install Deskside Server

The following section describes the installation of a server into a Deskside enclosure for installation in an office environment.

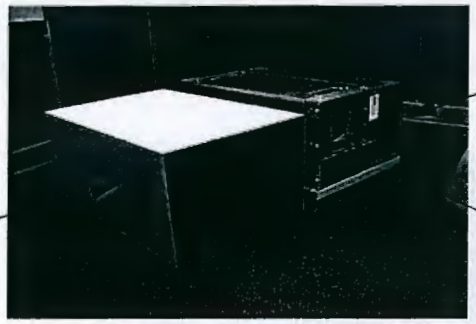
WARNING **The typical rp54xx system can weigh up to 68kg (150lbs). *HP recommends using an approved lifting device.***

- **Lift and move the server in accordance with all local safety regulations.**
- **Do not attempt to lift the server by the plastic handles on the top and side covers.**

Failure to follow these precautions can cause injury to personnel or damage to equipment.

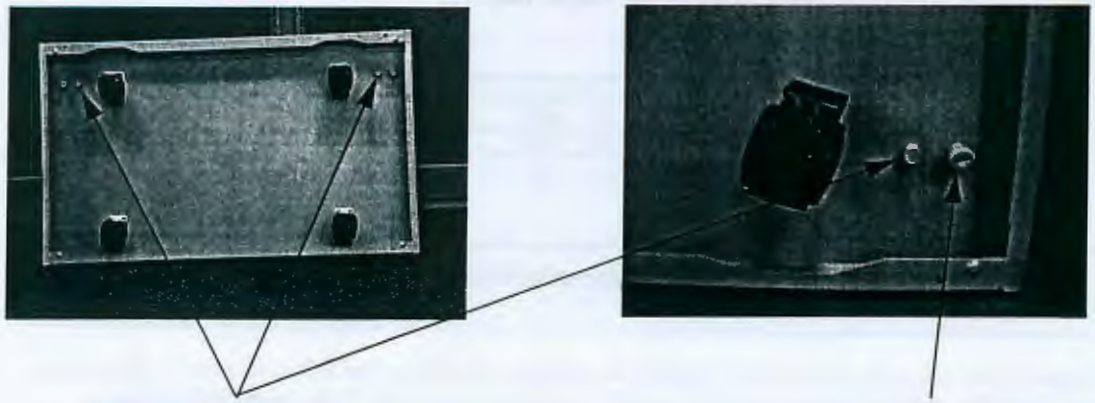
Step 1. Unpack the server.

Step 2. Unpack the deskside enclosure.



NOTE Ensure that the positioning spring pins in the enclosure base align with the alignment holes in the bottom of the server.

3155
2



Step 3. Position the server on the wheeled enclosure base.

Step 4. Tighten the two captive screws in the enclosure base to secure the server to the base.

Step 5. Position the enclosure cover (outside skin) over the server and install and tighten the screws to secure it to the base.

NOTE The perforations and the lip of the outside skin should be toward the rear of the server.

WARNING **Stacking rp54xx servers in deskside enclosures is *not* supported.**

Stacking rp54xx servers in deskside enclosures can damage equipment, may cause injury to personnel, and may void your warranty or service contract.

Step 6. Install the Front Bezel.

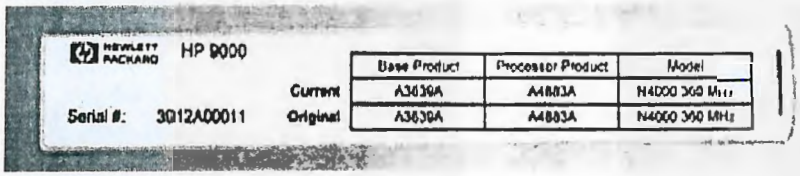
Step 7. Locate the two pull-tabs. One pull-tab is longer than the other. The shorter pull-tab is blank on both sides. The back of the shorter pull-tab provides a writable surface for Customer use.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0018
Fls:
3701
Doc:

3.154
2

Step 8. Locate the plastic bag containing the label sheet (taped to the server).

Step 9. Remove the label containing serial number, base product, processor product, and model information from the label sheet and apply to the back of the longer pull-tab.



NOTE Pull-tab and label shown above is for an rp74xx server. rp54xx uses the same style label and similar pull-tab.

Step 10. Insert the pull-tabs into the front bezel. Install the longer pull-tab in the left side plastic window in such a way that the rp54xx logo is visible. Install the shorter pull-tab in the right side plastic window with either surface visible. Refer to the diagram above for pull-tab locations.

3153
2

Install Stand-Alone Server in a Cabinet

The following describes how to install the A5556A slide-tray assembly into an approved HP cabinet in preparation for installing an rp54xx server.

This slide-tray assembly can be installed in an HP E-Series cabinet or other HP cabinets approved for rp54xx system installation. To install the A5556A slide-tray assembly in an approved HP equipment cabinet, proceed as follows:

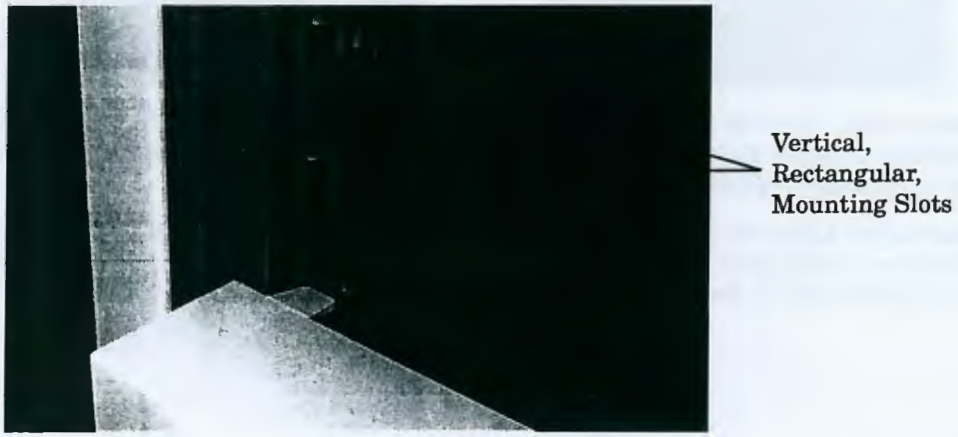
Step 1. Determine what type of cabinet you are installing the slide-tray assembly into.

a. E-Series cabinets have:

- Parchment white, plastic, sectional, side panels
- Black painted vertical frame posts with a partial return flange.

b. Approved, non-E-Series, cabinets have:

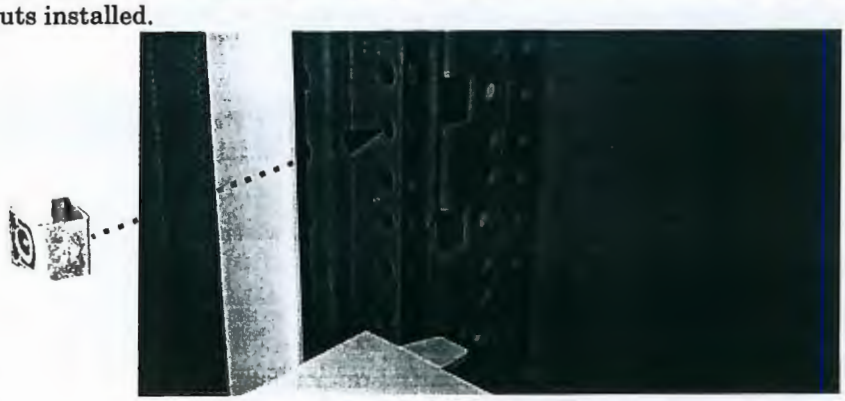
- Single piece metal side panels
- Gray painted verticle frame posts with full return flanges.



Step 2. Note the vertical, rectangular, slots in the return flanges on the vertical mounting posts. Determine into which of these vertical slots the slide/tray kit will be installed. This is done by counting down eight rectangular slots from the top of the cabinet or the bottom of the equipment above.

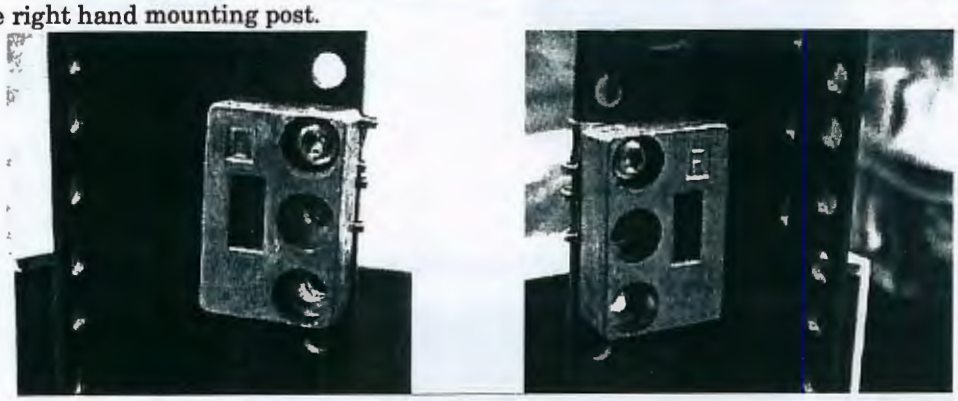
RQS Nº 03/2005 - CN
CPMI - CORREIOS
0019
Fls:
3701
Doc:

Step 3. On the front vertical mounting posts *only*, slide M5 sheet metal nuts onto the posts over the holes immediately adjacent to the vertical slots determined in the previous step. Also place M5 sheet metal nuts on the holes directly above these. Orient the sheet metal nuts so that the threaded portion faces towards the outside of the cabinet. There should now be a total of four (4) sheet metal nuts installed.



Step 4. If the cabinet is a non-E-Series cabinet, discard the left hand and right hand aluminum spacers and two of the M5 x 16 screws with cress-cup washers and proceed to step 12.

Step 5. If the cabinet is an E-Series cabinet, place the hook of the aluminum spacer marked "L" (5183-1864) into the appropriate vertical, rectangular slot on the front, left hand mounting post. The hook points downward. Similarly, place the spacer marked "R" (5183-1863) into the appropriate slot on the right hand mounting post.



Step 6. Use one M5 x 16 screw with cress-cup washer to attach each spacer to its vertical post. Do this by inserting the screw through the top hole in the spacer, through the mounting rail and tightening it into the sheet metal nut located at that position.

Step 7. Take the left hand slide/bracket assembly (marked 337079-1L) and install it into the left hand vertical mounting posts. This is done by inserting the pin at the rear of the slide's mounting bracket into the 23rd hole in the rear vertical mounting post and inserting the hook at the front of the

3151
2

bracket into the vertical, rectangular slot in the aluminum spacer. The slide should be positioned in the cabinet so that it is horizontal and level.

Step 8. Securely fasten the rear of the slide's mounting bracket to the rear vertical mounting post by installing and tightening two of the M5 x 16 screws with cress-cup washers thorough the mounting post, through the slides mounting bracket and into the threaded nuts attached to the mounting bracket.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 0020
Doc: 3701

Step 9. Fully extend the slide so that it is locked in the fully open position.

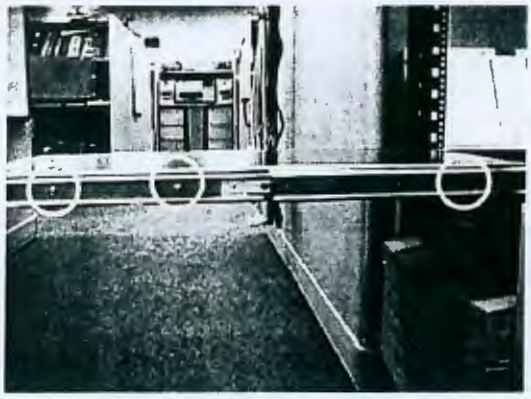
Step 10. Use an M5 x 30 screw with a cress cup washer to attach the front of the slide to the vertical mounting post. Insert the screw through the slide, through the center hole of the aluminum spacer, through the vertical mounting post, and tighten into the sheet metal nut located at that position.

Step 11. Use a procedure similar to steps 7 through 10 to install the right hand slide/bracket assembly (marked 337079-1R) and then proceed to step 12.

3 149
1

Step 12. Take the tray and place it onto the pins that extend from the slides' inner members. The slots with wide lead-in guides on the side of the tray fit down onto the slides' pins. The flat part of the tray will be on top, and the mounting holes in the top of the tray will be located to the right of the center of the tray. Slide the tray all the way down on both sides so that the pins reach the top of the slots in the side of the tray.

Step 13. Use six, M5 x 12 screws (without washers) to attach the tray to the slides. Three screws are used to attach each slide. Insert the screws through the slides, through the tray and tighten into the threaded nuts located on the inside of the sides of the tray.



3 Pan Head
M5x12 T25 screws
on each side

Step 14. From the bottom of the tray pull the plunger pin down and give it a 1/4 turn to hold it in place.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0021
Fls:
7 0 1
Doc:

EQT
3 148
L
CPL-A

Step 15. Position the server on the tray aligning the plunger pins with the alignment holes in the chassis.

Step 16. Release the plunger pins to secure the server.

3147
2
CPI - R.C.

Stationary L-Bracket Rail Assembly

rp54xx servers may be installed into E-Series and approved Non- E-Series cabinets using stationary L-bracket rail assembly kits listed below.

NOTE rp54xx servers are supported in Hewlett-Packard E-series and approved Non- E-series Hewlett-Packard cabinets, and approved rail kits.

For information on additional qualified 3rd party cabinets and rail kits, contact the nearest Hewlett-Packard Response Center.

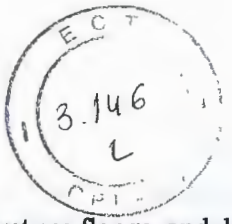
Cabinet Type	Rail Kit Product Number
E-Series HP Cabinet	A5575A
Other Approved HP Cabinet	A5562A

Identifying Approved Non-E-Series HP Cabinets

Approved Non- E-Series cabinets have black frames, one piece outside sheet metal skins, a partial return flange, and *requires* the installation of the aluminum spacer blocks, supplied with the rail kits.

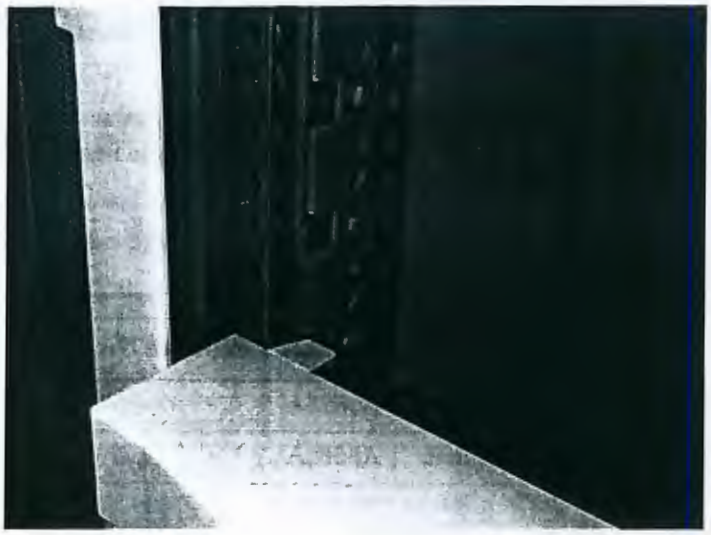
Approved Non- E-Series cabinets include the following product numbers: A1883A, A1884A, A1896A, A1897A, C1897A, C2785A, C2786A, and C2787A.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 0022
Doc: 3701



Identifying E-Series HP Cabinets

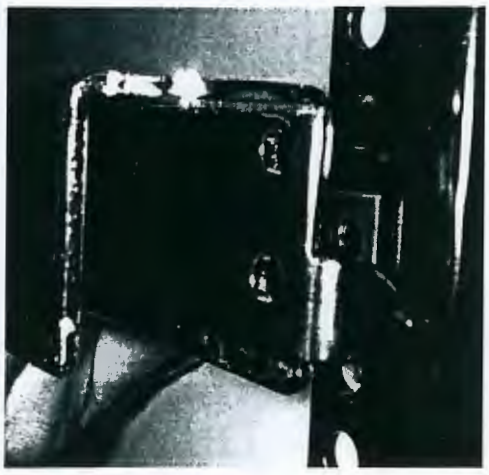
E-Series cabinets have light gray frames, sectioned, plastic outside "skins", a full return flange, and does *not* require the installation of the aluminum spacer block supplied, with the rail kits.



E-Series cabinets include the following product numbers: A5134A, A5136A, A5136A, A4900A, A4901A, A4902A, J1500A, J1502A, and J1502A.

Identifying Static Rail Kit

Hewlett-Packard has currently approved two static rail kits for use in cabinet mounting the rp54xx server. They are illustrated below.



A5562A Kit Rail

A5575A Kit Rail

3145
L

Installing Stationary Rails

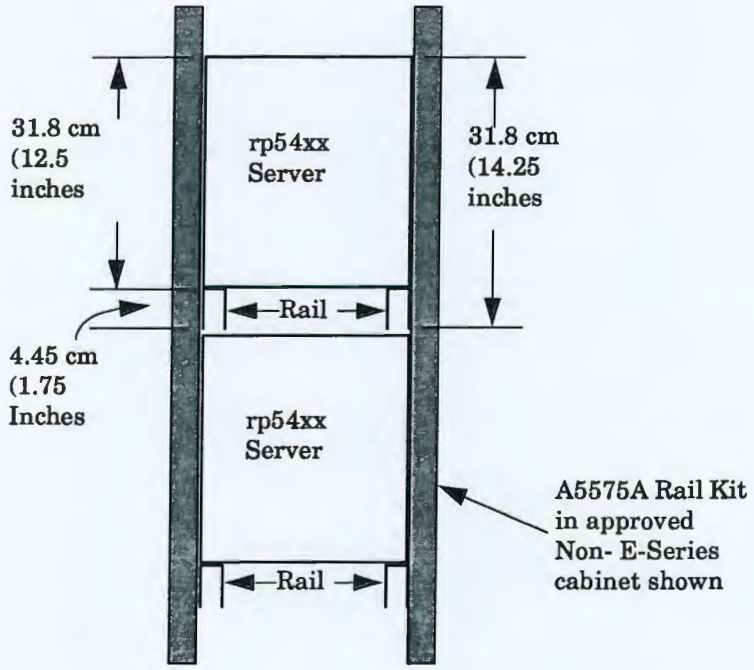
The installation of stationary rails is similar for most cabinet and rail combinations. The key considerations to are:

- Ensure that all safety precautions are read, understood, and observed
- Follow all installation instructions provided with the cabinet and rail kits, and
- Ensure that the rails extend out from the cabinet posts sufficiently to properly and safely support the equipment being installed.

To install an rp54xx server on stationary rails in an approved cabinet proceed as follows:

Step 1. Locate the rail mounting height in the cabinet. Allow for the following space requirements:

- For each rp54xx server, allow 31.8cm (12.5 inches) vertically (7 EIAs or Rack Units (RUs).
- If installing the A5575A rail kit, allow an *additional* vertical 4.45cm (1.75 inches (1 EIA) each set of rails.



Step 2. Install sheet metal nut(s) in the vertical cabinet posts at the required height for the kit being installed:

- Install the first nut either:
  - — 4.45 cm (1.75 Inches) above the top, or
  - — 31.8 cm (12.5 inches) below the bottom of the last server.
- If installing a A5562A rail kit, install the second nut in the next frame hole below the first.

Step 3. Hold the rail in place and insert and tighten the screws.

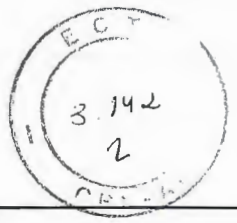
ROS Nº 03/2005 - CN
CPMI - CORREIOS
0023
Fls:
Doc: 3701

For installation of other qualified cabinet and rail combinations refer to the safety precautions and instructions accompanying them.

3. 143
2

3 Installing Additional Components

ROS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 0024
Doc: 3701



Additional Components

Some internal components are too delicate to be installed in the server prior to shipping. These internal components are shipped with the server, but are packed separately. They can be installed after the cabinet has been unpacked and positioned.

Some of the internal components that are packed separately are not user-installable. To maintain warranty validation, these items *must* be installed by a Hewlett-Packard Customer Engineer.

If you received either (or both) of the components listed below, contact your Hewlett-Packard provider to arrange for installation.

- Central Processing Units (CPUs)
- Power Distribution Units (PDUs)

Installing Memory

Memory Configuration Rules

rp54xx servers have 16 slots (8 DIMM pairs) for memory DIMMs. These slots are numbered 0a/b, 1a/b,... 7a/b. 8 of these slots (4a/b - 7a/b) are disabled on rp5400 servers. rp5450 servers can access all slots. rp5400 and rp5450 servers have DIMM slots located on the System Board.

rp5470 servers install DIMMs using Memory Carriers. The Memory Carriers fit into slots on the System Board.

The following rules govern the installation of memory DIMMs for rp5400, rp5450, and rp5470 servers:

- Memory must be installed in DIMM pairs.
- The capacity of DIMMs within a pair must be the same.

  Install DIMMs with the greatest capacity in the lowest slot numbers.
- Install DIMMs the following slot order: 0a/b, 1a/b, 2a/b, 3a/b, and so on.

Installing rp5400 and/or rp5450 DIMMs

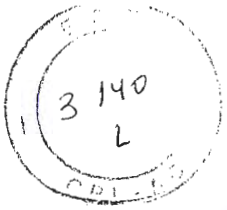
Step 1. Power down and *unplug* the rp54xx server.

CAUTION DC voltages are present when the server is connected to AC power. Do not install or service rp54xx internal components while DC voltage is present. Failure to observe this precaution can result in damage to the server.

Step 2. Loosen the captive T-15 screws that hold the top cover in place, then grasp the strap handle, raise the cover slightly, and pull the cover toward the front of the server to free the cover tabs from the slots in the chassis. The air baffle will be exposed.

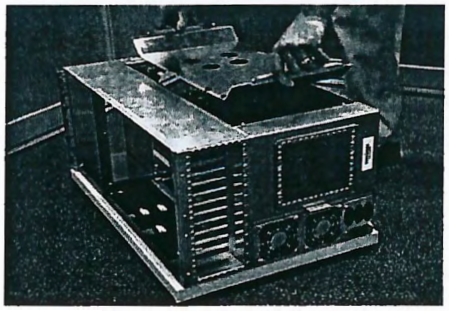
Step 3. Make the top of the server accessible for service.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0025
Fls:
Doc: 3701



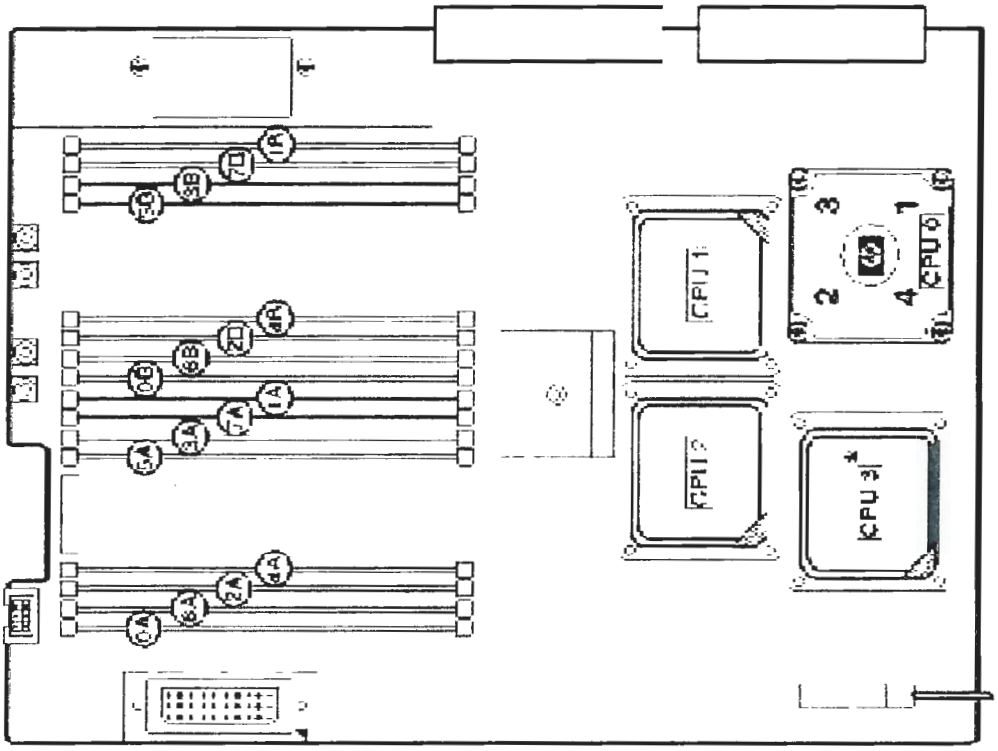
Step 4. Loosen the captive T-15 screws on the air baffle. Grasp the two handles on the baffle, and lift the baffle remove it.

CAUTION Observe all ElectroStatic Discharge (ESD) precautions Do not touch internal components. Failure to observe ESD precautions can cause damage to components.



Step 5. Observe Electrostatic Discharge (ESD) precautions.

Step 6. Refer to the following graphic for memory slot locations.



3139

Locate the correct DIMM pair slots. Insert the DIMM connectors into the guides until the card snaps firmly in place. It may be necessary to apply downward force using the palm of your hand on the DIMM. Observe the top of the DIMM to make sure one side is not higher than the other.

NOTE It may be necessary to remove PSM 1 when installing a DIMM in slot 0a and PSM 0 when installing a DIMM in slot 1b. If either PSM is removed to install memory, ensure it is re-installed.

Step 7. Replace the air baffle. Tighten the four captive screws to secure the air baffle in place.

Step 8. Replace the top cover. Tighten the four captive screws to secure the top cover in place.

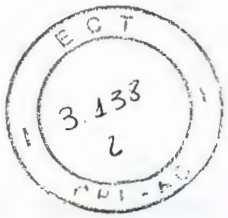
Step 9. For rack configurations, insert the rp54xx server back into the rack.

Step 10. For deskside enclosure configurations, replace the deskside enclosure cover.

Step 11. Power the rp54xx server on.

Step 12. Use the BCH command `in me` to verify the system recognizes the memory that you have just added.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0026
Fls:
3701
Doc:



Installing rp5470 DIMMs

DIMMs for the rp5470 system are installed in memory carriers instead of the system board, as are the other rp54xx systems. However, rp5470 memory carriers are also located on the system board, so the method for opening and closing the system is the same. Procedures for removing and replacing the server top and baffle are listed below, without the pictures shown in the section titled, *"Installing rp5400 and/or rp5450 DIMMs."* If you wish to reveiw the pictures, please refer to the aforementioned section.

Step 1. Power down and unplug the rp54xx server.

NOTE DC voltages are present when the server is connected to AC power. Do not attempt to install or service: CPUs, Memory, PSMs, the Platform Monitor or PCI I/O cards installed in non-Turbo slots (1-6) while DC voltage is present. Failure to observe this warning may result in damage to the server.

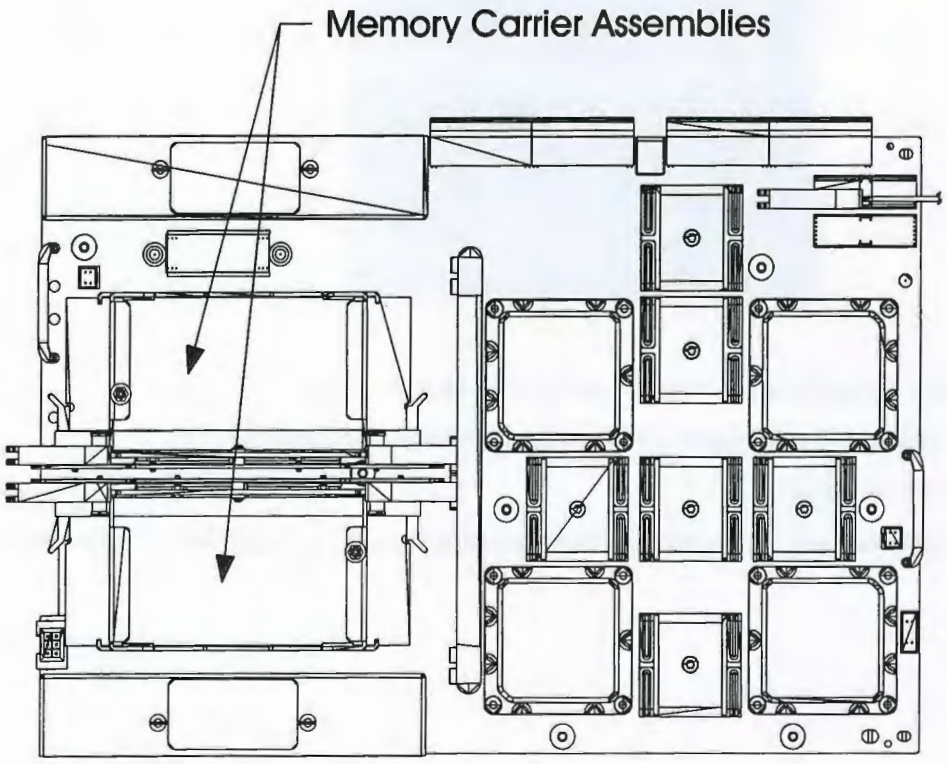
Step 2. Make the top of the server accessible for service.

Step 3. Loosen the captive T-15 screws that hold the top cover in place, then grasp the strap handle, raise the cover slightly, and pull the cover toward the front of the server to free the cover tabs from the slots in the chassis. The air baffle will be exposed.

Step 4. Loosen the four (4) captive T-15 screws on the air baffle. Grasp the two handles on the baffle, and lift and remove the baffle.

Step 5. Observe Electrostatic Discharge (ESD) precautions.

Step 6. Refer to the following graphic for Memory Carrier locations.



3.13.7
2

a. Locate the Memory Carrier and pull up on the extractor levers on each end of the Memory Carrier to unseat the Memory Carrier from its socket.

b. When the Memory Carrier unseats from the socket, pull it away from the System Board.

c. Loosen the captive screws that secure the DIMM Clip and remove the DIMM Clip from the Memory Carrier.

d. Seat the memory DIMM into its socket on the Memory Carrier.

e. Press the extractor levers on each end of the memory DIMM slot inward until the levers snap into place.

f. Attach the Memory Clip to the Memory Carrier with the DIMM slot markings on the top of the Memory Clip aligned with the DIMM slot markings on the Memory Carrier.

g. Secure the Memory Clip using the captive screws.

h. Seat the Memory Carrier into the appropriate slot on the System Board.

i. Push down on the extractor levers and snap them into place.

tep 7. Replace the air baffle. Tighten the four captive screws to secure the air baffle in place.

Step 8. Replace the top cover. Slide the cover tabs into the slots in the chassis and close the cover. Tighten the two captive screws to secure the top cover in place.

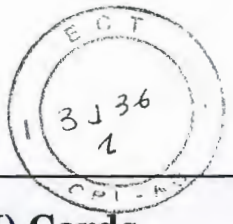
Step 9. For rack configurations, insert the rp54xx server back into the rack.

Step 10. For deskside enclosure configurations, replace the deskside enclosure cover.

Step 11. Power the rp54xx server on.

Step 12. Use the BCH command `in me` to verify the system recognizes the memory that you have just added.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0027
Fls:
Doc: 3701



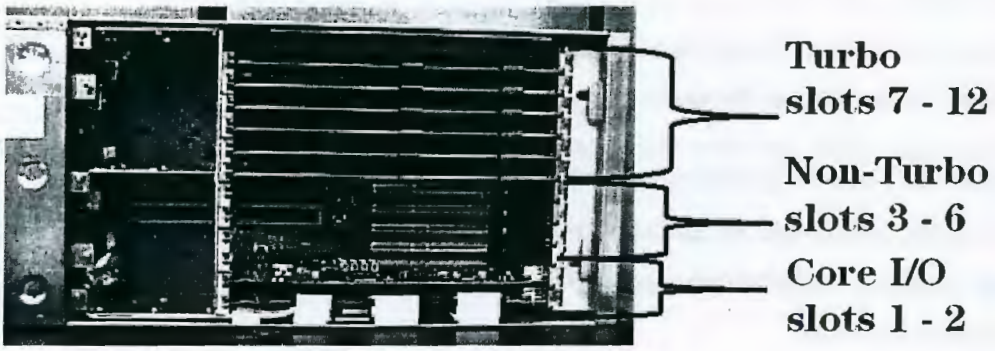
Installing Peripheral Component Interconnect (PCI) Cards

rp54xx servers have a total of 12 PCI I/O slots. Slots 1 and 2 are reserved for the LAN/SCSI and GSP Core I/O cards, leaving 10 PCI I/O slots available for Customer use.

rp5400/rp5450 PCI Card Slots

For rp5400 and rp5450 models, 10 PCI I/O slots consist of Turbo and non-Turbo slots. Server PCI slots are shown below.

rp5400/rp5450 PCI Card Slots



- Slots 1 and 2 are reserved for the rp54xx LAN/SCSI and GSP (Guardian Service Processor) Core I/O cards, respectively. Slots 1 and 2 are non-Turbo slots. Non-Turbo slots share a single 250MB/s PCI bus and are incapable of HotPlug functionality. The server must be turned off prior to removing or installing the LAN/SCSI or GSP cards in these slots.
- Slots 3 - 6 are non-Turbo slots. These four Non-Turbo slots share a single 250MB/s PCI bus, run at 33MHz and support 32 and 64-bit PCI cards. Non-Turbo slots are incapable of HotPlug functionality. The server must be turned off prior to removing or installing PCI cards in these slots.
- Slots 7 - 12 are Turbo slots. Each Turbo slot has a dedicated 250MB/s PCI bus, run at 66MHz and support 32 and 64-bit PCI cards. Turbo slots are HotPlug capable. Below each Turbo slot is a plastic PCI card separator. The PCI card separator has two LEDs and a pull tab on the outer edge. The LED's provide power and status for the slot. The pull tab allows the PCI card to be easily removed.

rp5400 servers have access to slots 1, 2 and 8-12 while rp5450 servers have access to all (1-12) slots.

NOTE Slot 3 will become enabled on rp5400 servers with server firmware versions later than 40.48.

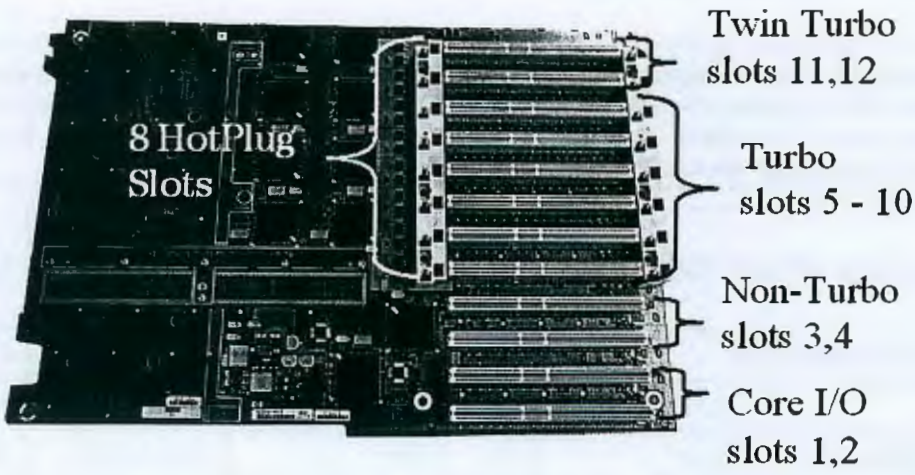
A slot 3 enabled label (A5576-84009) is available for rp5400 systems.

3.135
L

rp5470 PCI Card Slots

For rp5470 models, the 10 PCI I/O slots consist of Twin Turbo, Turbo, and non-Turbo slots. The following illustration shows the PCI card slot layout.

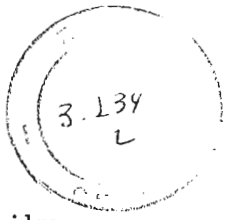
rp5470 PCI Slots



- Slots 1 and 2 are reserved for the rp54xx LAN/SCSI and GSP (Guardian Service Processor) Core I/O cards, respectively. Slots 1 and 2 are non-Turbo slots. Non-Turbo slots share a single 250MB/s PCI bus and are incapable of HotPlug functionality. The server must be turned off prior to removing or installing the LAN/SCSI or GSP cards in these slots.
- Slots 3 and 4 are non-Turbo slots. These two Non-Turbo slots share a single 250MB/s PCI bus, run at 33MHz and support 32 and 64-bit PCI cards. Non-Turbo slots are incapable of HotPlug functionality. The server must be turned off prior to removing or installing PCI cards in these slots.
- Slots 5 - 10 are Turbo slots. Each Turbo slot has a dedicated 250MB/s PCI bus, run at 66MHz and support 32 and 64-bit PCI cards. Turbo slots are HotPlug capable. Below each Turbo slot is a plastic PCI card separator. The PCI card separator has two LEDs and a pull tab on the outer edge. The LED's provide power and status for the slot. The pull tab allows the PCI card to be easily removed.
- Slots 11 and 12 are Twin Turbo slots. Each Twin Turbo slot has a dedicated 500MB/S PCI bus, runs at 66 MHz, and supports 32- and 64-bit PCI cards. Twin Turbo slots are HotPlug capable. Below each Twin Turbo slot is a plastic PCI card separator. The PCI card separator has two LEDs and a pull tab on the outer edge. The LED's provide power and status for the slot and the pull tab allows the PCI card to be easily removed.

rp5470 servers have access to all (1-12) slots.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 0028
Doc: 3791



PCI I/O Card Installation Restrictions

Restrictions apply regarding the installation of PCI I/O cards which contain a PCI-to-PCI bridge:

- HP-UX boot is currently not supported for cards that contain a PCI-to-PCI bridge.
- HP-UX patches are required when more than one card containing a PCI-to-PCI bridge is installed in non-Turbo slots.

PCI I/O Card Installation Order

The following table shows a standard factory PCI card installation that begins with slot 12. Use this table as a guideline for installing PCI I/O cards in the field.

NOTE A system shipped from the factory may have a different configuration than the same system built in the field. For example: The factory will install the graphics card in slot 12 and add other cards below. In the field, slot 12 may already be occupied by another PCI card. It is acceptable for the graphics card to be installed in any available Turbo slot.

Product Number	Description (all are PCI cards)	Max	Boot	Load Order *	Part Number	Notes
A6150A	Graphics, Graphics Card	1	No	1	A4982-66501	3,8
A5838A	Combo		No	3	A5838-60001	9
A5483A	ATM 622Mbps MMF Adapter	10	No	4	A5483-60001	10
A4926A	1000Base SX PCI LAN Adapter	10	No	5	A4926-60001	
A4926A	1000Base TX PCI LAN Adapter	10	No	6	A4926-60001	
A6092A	HYPERFabric		No	7	A6092-60001	11
A5158A	FC Taclite		Y	8	A5846-60001	
A5486A	Praesidium Speed Card	10	No	9	A5486-60001	
A5506A	4 Port 100Base TX LAN Adapter	7/10	No	10	A5506-60101	1,2,6
A5506B	4 Port 100Base TX LAN Adapter	7/10	No	10	A5506-60102	
A5150A	Dual Port Ultra 2 SCSI adapter	10	Yes	11	A5150-60001	4
A5149A	Single Port Ultra 2 SCSI HBA	10	Yes	12	A5149-60001	
J3526A	High Perf 4 Ports Synchronous Adapter	10	No	13	5063-1322	7,5
A4800A	FWD SCSI-2 adapter	10	Yes	14	A4800-67002	
A5230A	100Base-T LAN Adapter	10	No	15	B5509-66001	
A3738A	10/100Base-T LAN Adapter	10	No	16	A3738-60001	
A3739A	Dual FDDI LAN Adapter	10	No	17	A3739-60001	
A5783A	Token Ring 4/16/100 Hardware Adapter	10	No	18	A5783-60101	

3.133
2

Product Number	Description (all are PCI cards)	Max	Boot	Load Order *	Part Number	Notes
J3525A	Dual Port Synchronous Adapter	10	No	19	J3525-60001	
J3593A	64 port Serial MUX system card	10	No	20	J3593-60001	
J3592A	8 Port PCI Serial MUX card	4	No	21	J3592-60101	
A6150A	Graphics, USB Card	1	No	22	A6150-60001	
A6150BX	Pinnacle 2 Graphics	1	No	1	A6150-60003	12,13
A6386A	Hyper Fabric 2 Interconnect	10	No	6	A3686-60001	
A5506A	Quad Port 10/100B-TX LAN	10	No	10	A5506-60102	14
A6749A	3.3v 64 Port Terminal MUX	10	No	24	A6749-60001	
A6748A	3.3v 8 Port Terminal MUX	10	No	25	A6748-60001	

*In top down order.

Notes:

1. Card contains a PCI-to-PCI bridge.
2. Requires PHKL_20123, PHKL_20629 and PHNE_19826 or their superseded equivalents.
3. Not supported in non-Turbo slots. Install in Turbo slots only.
4. Requires server firmware revision 39.46 or later.
5. Requires HP-UX 11.1
6. Maximum is 7 for HP-UX versions prior to 11.0. Maximum is 10 for HP-UX version 11.1 and later.
7. Requires PHKL_19543 and PHKL_19544 or their superseded equivalents.
8. Requires HP-UX 11.0 Support Plus (IPR) 0006, June 2000 or later. This product to be released 6/00.
9. Not supported in a shared slot (slots 3-4 for rp5470, slots 3-6 for rp5450, not applicable for rp5400).
10. If you are installing ATM 622 cards in an rp5470 configuration, do not install them in slots 3 and 4 (shared slots).
11. Requires 768 MB for first card and 512 MB for each additional card.
12. Not supported in shared slots.
13. Max of 1. Needs USB card for keyboard and mouse.
14. Contains PCI bridge.

ROS Nº 03/2005 - CN
CPMI - CORREIOS
0029
Fls:
Doc: 701

Installing a PCI Card

Follow these procedures to install a PCI card.

Step 1. Power down and unplug the rp54xx server.

NOTE DC voltages are present when the server is connected to AC power. Do not attempt to install or service: CPUs, Memory, PSMs, the Platform Monitor or PCI I/O cards installed in non-Turbo slots (1-6) while DC voltage is present. Failure to observe this warning may result in damage to the server.

Step 2. Make the right side of the server accessible for service.

Step 3. Using a Torx 15 screwdriver, loosen the captive screws on the right side panel. This panel has a label which shows which PCI I/O slots are available and the corresponding paths. The PCI I/O slot paths for rp5400, rp5450, and rp5470 are shown below.

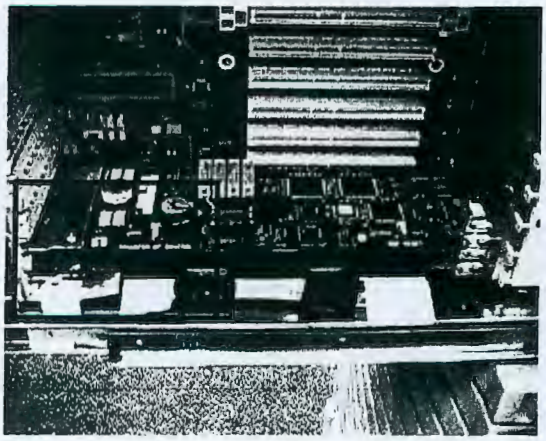
Slot	rp5400		rp5450		rp5430/rp5470	
	Slot Type	**Path**	**Slot/Type**	**Path**	**Slot Type**	**Path**
12	**Turbo**	**0/4/0**	**Turbo**	**0/4/0**	**Twin Turbo**	**0/10/0**
11	Turbo	0/7/0	Turbo	0/7/0	Twin Turbo	0/12/0
10	Turbo	0/3/0	Turbo	0/3/0	Turbo	0/8/0
9	Turbo	0/6/0	Turbo	0/6/0	Turbo	0/9/0
8	Turbo	0/2/0	Turbo	0/2/0	Turbo	0/3/0
7	Not Available		Turbo	0/5/0	Turbo[a]	0/1/0
6	Not Available		Shared	0/1/0	Turbo[a]	0/5/0
5	Not Available		Shared	0/1/1	Turbo[a]	0/2/0
4	Not Available		Shared	0/1/2	Shared[a]	0/4/0
3	Not Available[b]		Shared	0/1/3	Shared	0/4/2
2	GSP		GSP		GSP	
1	LAN/SCSI		LAN/SCSI		LAN/SCSI	

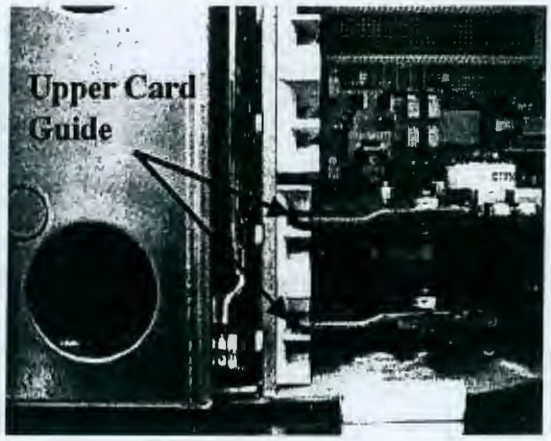
a. Slot is NOT AVAILABLE for rp5430.
b. Slot 3 becomes available with server firmware versions later than 40.48.

Step 4. Remove the PCI slot cover from the slot that will receive the PCI card. To remove the PCI slot cover, slide the PCI slot cover away from the server.

E.C.T. 3.131 2 C.P.I.-A.C.

Step 5. Slide the PCI card connectors into the slot, snapping firmly in place. For full length (cards that extend to the left side card guides) PCI cards, use the UPPER card guide.



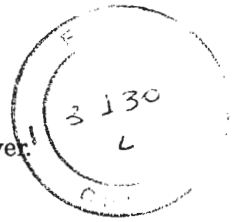


Step 6. At the rear of the chassis, connect the I/O cable to the card just installed.

Step 7. Replace the right side panel and tighten the captive screws.

Step 8. For rack configurations, insert the rp54xx server back into the rack.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0030
Fls:
3701
Doc:



Step 9. For deskside enclosure configurations, replace the deskside enclosure cover.

Step 10. Power the server on.

Step 11. Use the server firmware `in io` command to verify the PCI cards are recognized by the server. If AUTOBOOT is ON, it will be necessary to interrupt the boot process to get to the server firmware `Main Menu: Enter command or menu >` prompt.

Step 12. Boot HP-UX and run the `ioscan` utility to verify the system recognizes the new PCI card.

Online Addition/Replacement (OLA/R) of PCI I/O cards

Beginning with HP-UX 11i (11.11) rp54xx servers support the on-line addition and replacement of PCI I/O cards. In order for this high availability feature to be fully implemented, the following server requirements must be met:

- rp5400A/rp5450A firmware must be later than 40.26 (rp5400B/rp5450B/rp5470A firmware will support OLA/R upon its release).
- HP-UX operating system must be 11i (11.11) or later.

There is a bit that the HP-UX operating system examines to determine if the server hardware and firmware is capable of OLA/R. This bit is controlled by server firmware. If the bit is ON, OLA/R is possible (when requirements have been met). The bit was mistakenly set to ON for all rp5400 and rp5450 revision A (rp5400A and rp5450A) servers. As a result, HP-UX may incorrectly identify these models as being OLA/R capable. In order to avoid this confusion, verify that the correct level of server firmware is installed.

3.129
L-

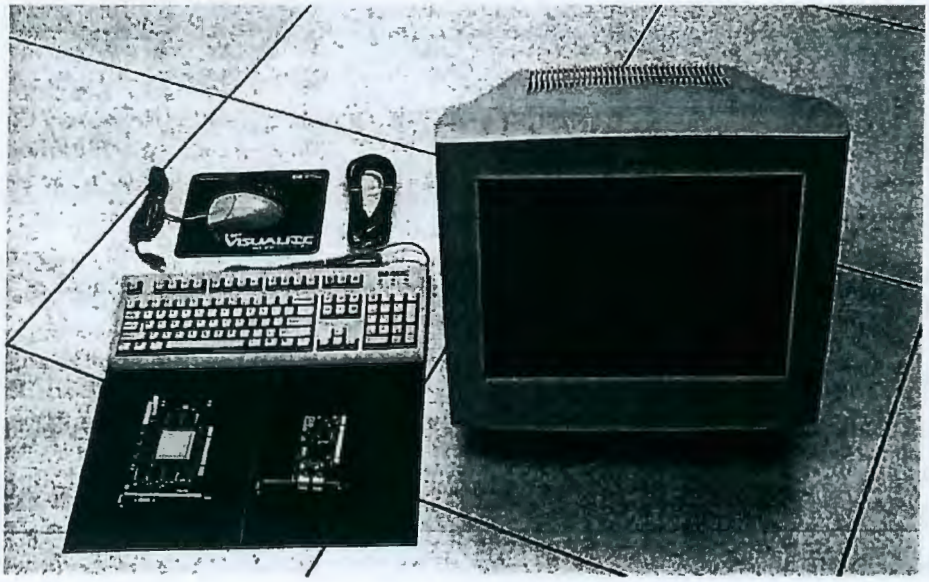
Installing Graphics

This section explains how to install rp54xx 2D graphics hardware. For a complete graphics solution, three products are required. The products listed below are the only products supported on rp54xx servers.

- A6150A rp54xx Graphics Package
  - — Includes PCI graphics card
  - — Includes PCI USB (Universal Serial Bus) card
- A4983B Keyboard and Mouse Kit
  - — Includes mouse with 114" cable
  - — Includes keyboard with 109" cable
- D8910W (19") or D2847W (21)" Monitor
  - — Includes localized power cord and 75" 15-pin video cable

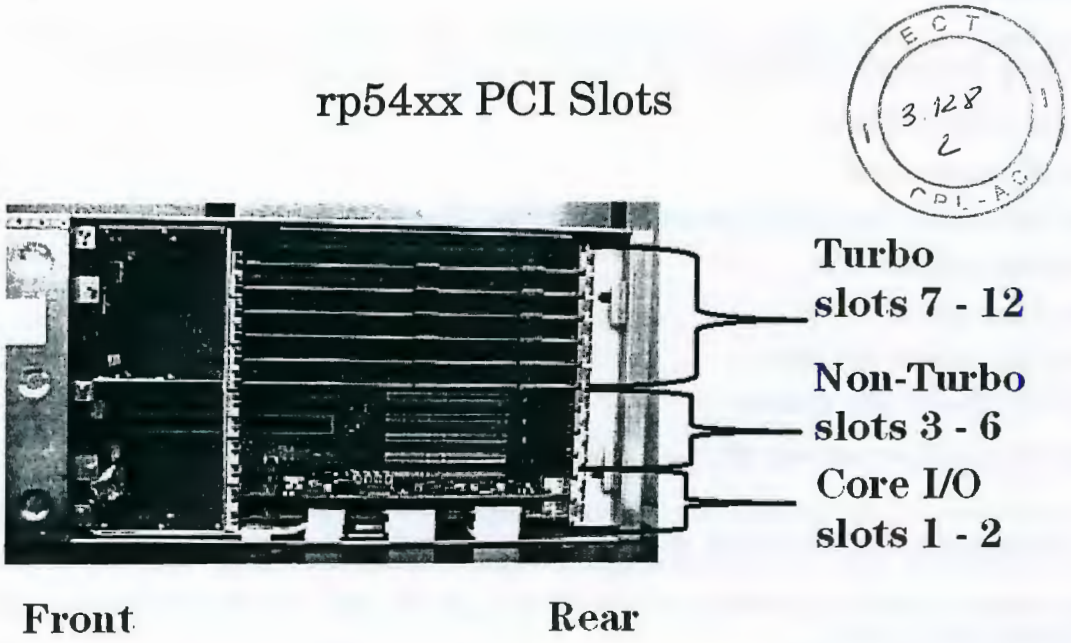
NOTE rp54xx graphics requires HP-UX 11.0 Support Plus (IPR) 0006, June 2000 or later.

The photo below includes the A6150A, A4983B and D8910W products. The video cable for the monitor is not shown. Black ESD mat not included.



RQS Nº 03/2003 - CN
CPMI - CORREIOS
Fls: 0031
Doc: 2701

rp54xx servers have a total of 12 PCI I/O slots. Slots 1 and 2 are reserved for the LAN/SCSI and GSP Core I/O cards, leaving 10 PCI I/O slots available for Customer use. These 10 PCI I/O slots consist of Turbo and non-Turbo slots.



- Slots 1 and 2 are reserved for the rp54xx LAN/SCSI and GSP (Guardian Service Processor) Core I/O cards, respectively. Slots 1 and 2 are non-Turbo slots. Non-Turbo slots share a single 250MB/s PCI bus. Non-Turbo slots are incapable of HotPlug functionality. The server must be turned off prior to removing or installing the LAN/SCSI or GSP cards in these slots.
- Slots 3 - 6 are non-Turbo slots. These four Non-Turbo slots share a single 250MB/s PCI bus, run at 33MHz and support 32 and 64-bit PCI cards. Non-Turbo slots are incapable of HotPlug functionality. The server must be turned off prior to removing or installing PCI cards in these slots.
- Slots 7 - 12 are Turbo slots. Each Turbo slot has a dedicated 250MB/s PCI bus, run at 66MHz and support 32 and 64-bit PCI cards. Turbo slots are HotPlug capable. Below each Turbo slot is a plastic PCI card separator. The PCI card separator has two LEDs and a pull tab on the outer edge. The LED's provide power and status for the slot. The pull tab allows the PCI card to be easily removed.

rp5400 servers can access PCI slots 1,2 and 8-12. rp5450/3000 servers can access all PCI slots.

Follow these procedures to install graphics cards.

Step 1. Install HP-UX 11.0 Support Plus (IPR) 0006, June 2000 or later. This step ensures the appropriate HP-UX drivers are installed.

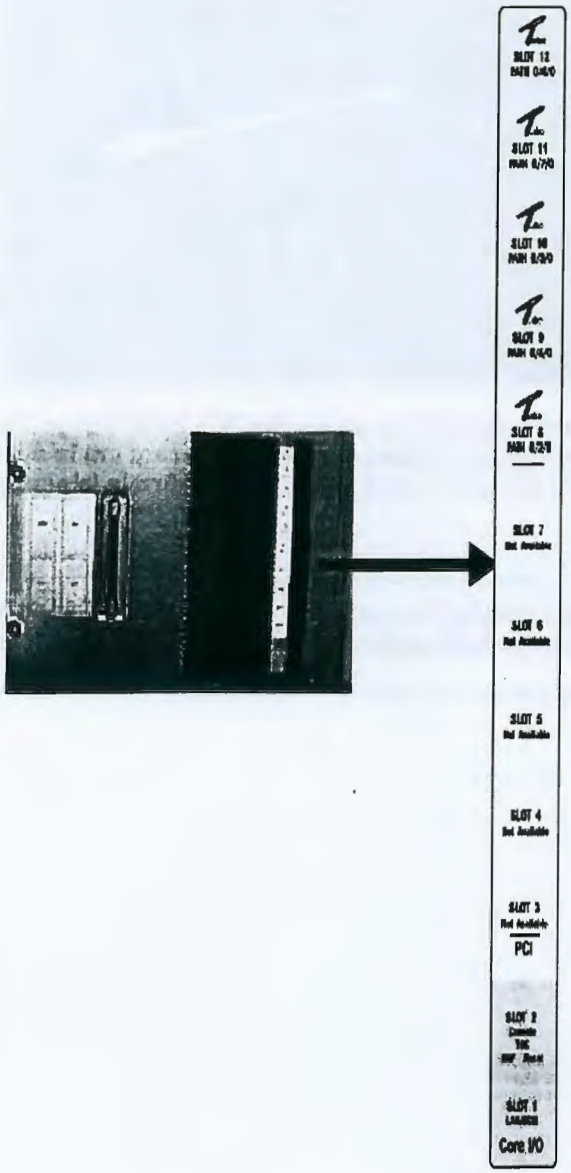
Step 2. Power down and unplug the rp54xx server.

3 127
2.

NOTE DC voltages are present when the server is connected to AC power. Do not attempt to install or service: CPUs, Memory, PSMs, the Platform Monitor or PCI I/O cards installed in non-Turbo slots (1-6) while DC voltage is present. Failure to observe this warning may result in damage to the server.

Step 3. Make the right side of the server accessible for service.

Step 4. Using a Torx 15 screwdriver, loosen the captive screws on the right side panel. This panel has a label which shows which PCI I/O slots are available and the corresponding paths. The label shown below is for an rp5400.



RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 0032
Doc: 2701

E.C.T.
3.126
2

Step 5. Grasp the handle on the right rear panel and remove the panel from the side of the chassis. The 12 PCI slots, numbered 1-12 from bottom to top, will be in view.

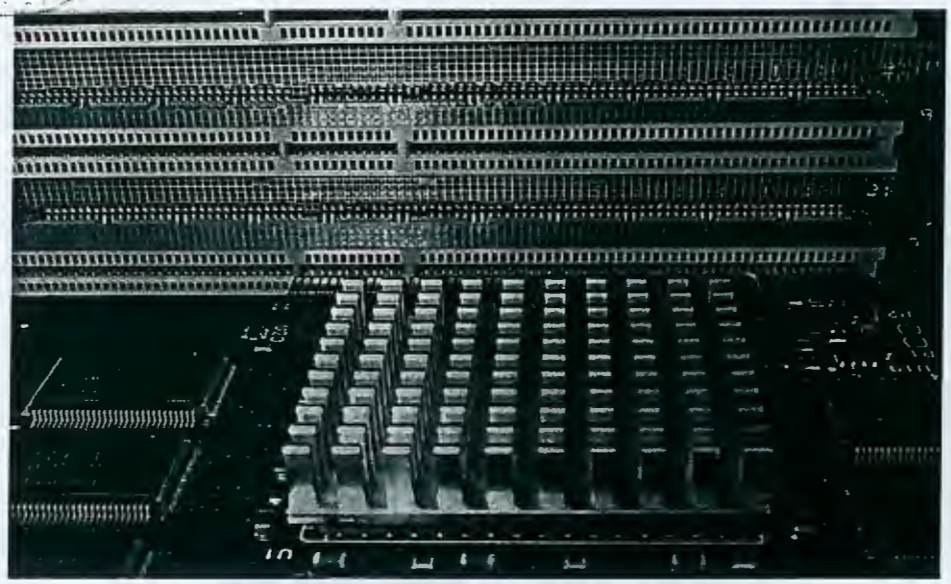
Step 6. Remove the PCI slot cover from the slot that will receive the PCI card. To remove the PCI slot cover, slide the PCI slot cover away from the server.

Step 7. Center the graphics card within the space created by removing the PCI I/O slot cover. Slide the card toward the edge connectors. Ensure the edge connectors on the card are in alignment with the connectors of the slot. Apply pressure to the card until it snaps firmly in place. Repeat process for USB card.

NOTE The graphics card must be installed in any Turbo slot while the USB will work in any slot. To reserve Turbo slots for high performance I/O cards, install the USB card in a non-Turbo slot

---

3.125
2



Step 8. At the rear of the chassis, connect the keyboard and mouse cables to the USB card. It does not matter which connector is used for the keyboard or mouse.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0033
Fls:
Doc: 3701

ECT
3.124
L
CPL-1

Step 9. Connect one end of the 15-pin video cable connector on the graphics card. This connector is labeled "Graphics Display" and "Video Out". Connect the other end of this cable to the graphics monitor.

Step 10. Replace the right side panel and tighten the captive screws.

Step 11. For rack configurations, insert the rp54xx server back into the rack.

Step 12. For deskside enclosure configurations, repalce the deskside enclosure cover.

Step 13. Power the server on.

3.123
L

Step 14. Use the server firmware `in io` command to verify the graphics cards are recognized by the server. If AUTOBOOT is ON, it will be necessary to interrupt the boot process to get to the server firmware `Main Menu: Enter command or menu >` prompt.

Step 15. Boot HP-UX and run the `ioscan` utility to verify the system recognizes the new PCI card.

Step 16. Logon as root and install X/CDE/Motif if not already installed.

Graphics Troubleshooting

This section describes how to troubleshoot common problems encountered during installation or attempted use of graphics. The following system utilities can be used to display or set the graphics configuration:

- `/opt/graphics/common/bin/graphinfo` allows you to display the current graphics configuration and the graphics drivers that are being used.
- `/opt/graphics/common/bin/setmon` allows you to reconfigure the monitor type.
- The `display` menu of the HP-UX System Administration Manager (SAM) utility allows you to configure the X-Server and set the monitor type.

  On-line diagnostics provide information, verify and diagnose coverage for the graphics and USB cards.Off-line diagnostics do not exist for either the graphics or USB card.
- The HP-UX `ioscan` utility can be used to verify the HP-UX operating system recognized the hardware.

Symptom: CDE will not come up.

Step 1. Ensure /dev/crt was created. If not created, use `insf -e` to create.

Step 2. Ensure the system is at run level 3. Use `who -r` to determine run level. Use `init 3` to change to run level 3.

Step 3. Ensure dt is enabled. Use `/usr/dt/bin/dtconfig -e` to enable dt.

Step 4. Ensure /etc/dt/config/Xservers exists. If not, use `/usr/dt/config/dtrc.d/20_graph_conf` to create.

Step 5. Ensure the line: * Local local@console /usr/bin/X11/X :0 is not commented out of the /etc/dt/config/Xservers file.

Step 6. Reboot HP-UX.

Symptom: HP-UX does not recognize the graphics cards. `unknown` **appears in the ioscan output for these cards**

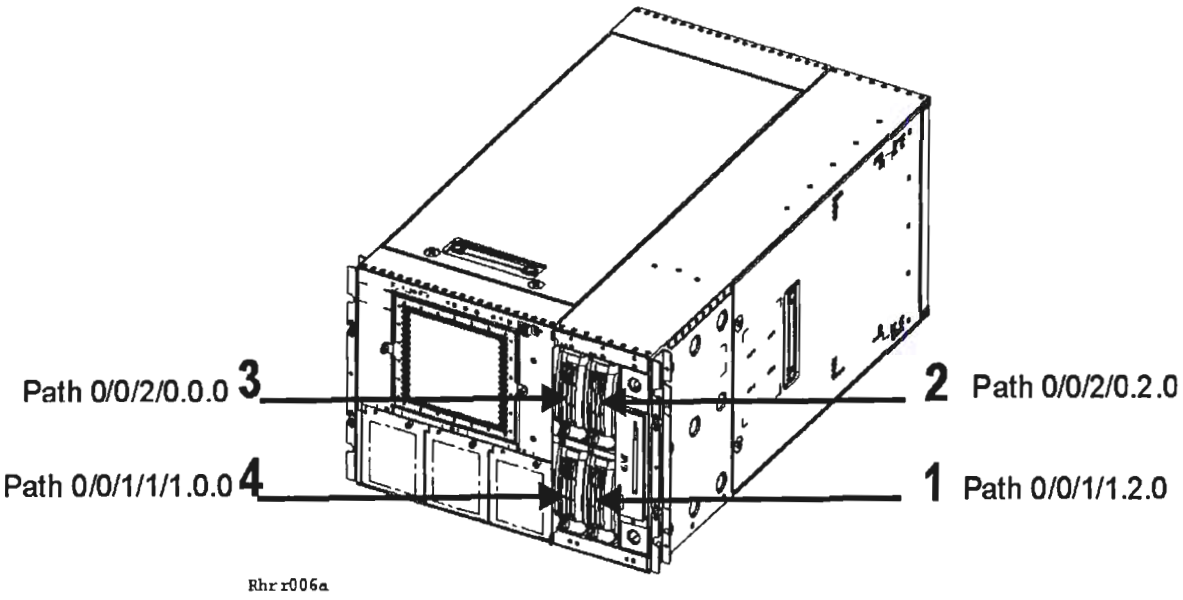
Step 1. Examine the output of the `swlist` command to ensure the correct version of HP-UX is installed.

Step 2. Update HP-UX as necessary

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0034
Fls:
Doc: 2701

Installing Disk Drives

rp54xx servers support up to four optional internal hard drives. These drives must be installed in the following sequence:

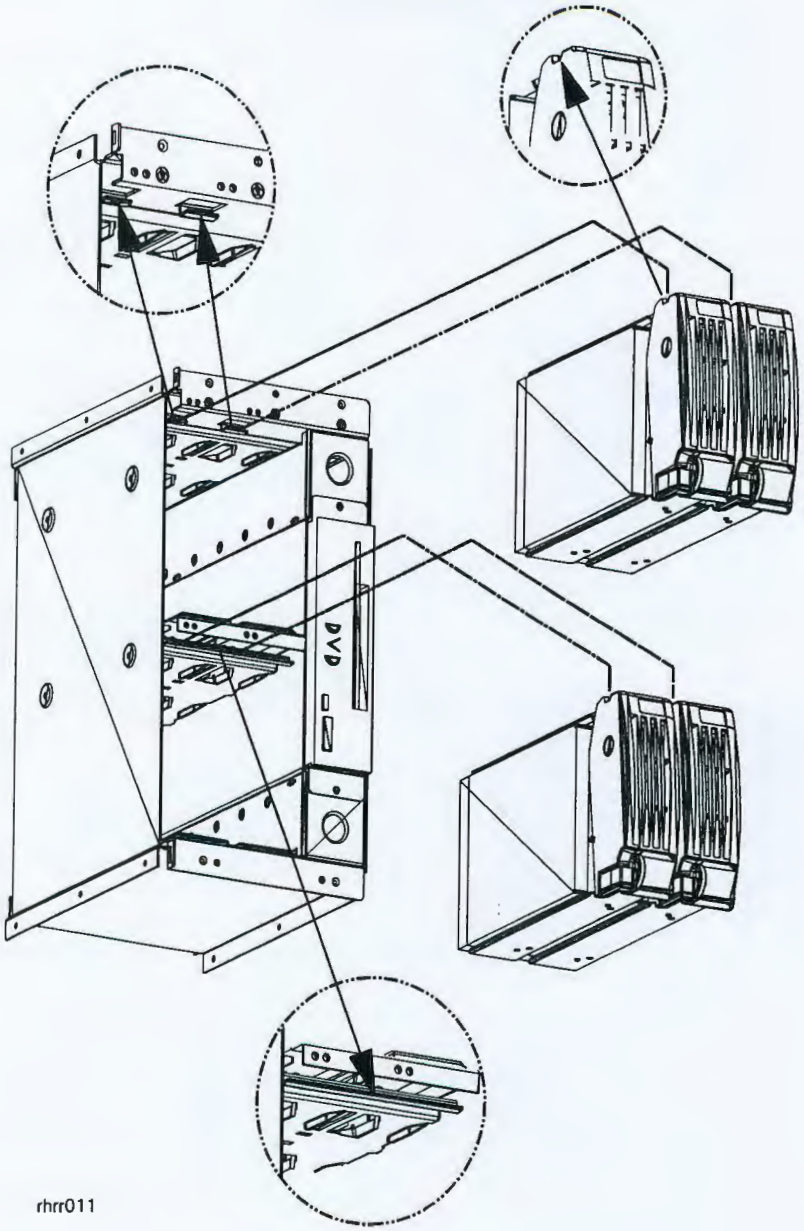


It is not necessary to shutdown the HP-UX operating system or power off the server to install a new disk. Follow this procedure to add internal hard disk drives to your rp54xx server.

Step 1. If a front bezel is installed on the face of the server, open the right-hand panel to gain access to the disk slots.

Step 2. Remove the disk drive slot cover.

Step 3. Insert the new disk drive into the slot until the rear connectors snap into place in the card guide. As shown in the following graphic, the notches at the top of the disk drives must snap over the small brackets in the disk bay to ensure a firm connection.



Step 4. Secure the connection by pushing the blue release lever closed.

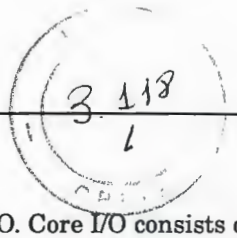
Step 5. Refer to HP-UX documentation to configure the new disk.

3120
L

ECT
3119
L

4 Cable Connections

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0036
Fls:
3701
Doc:

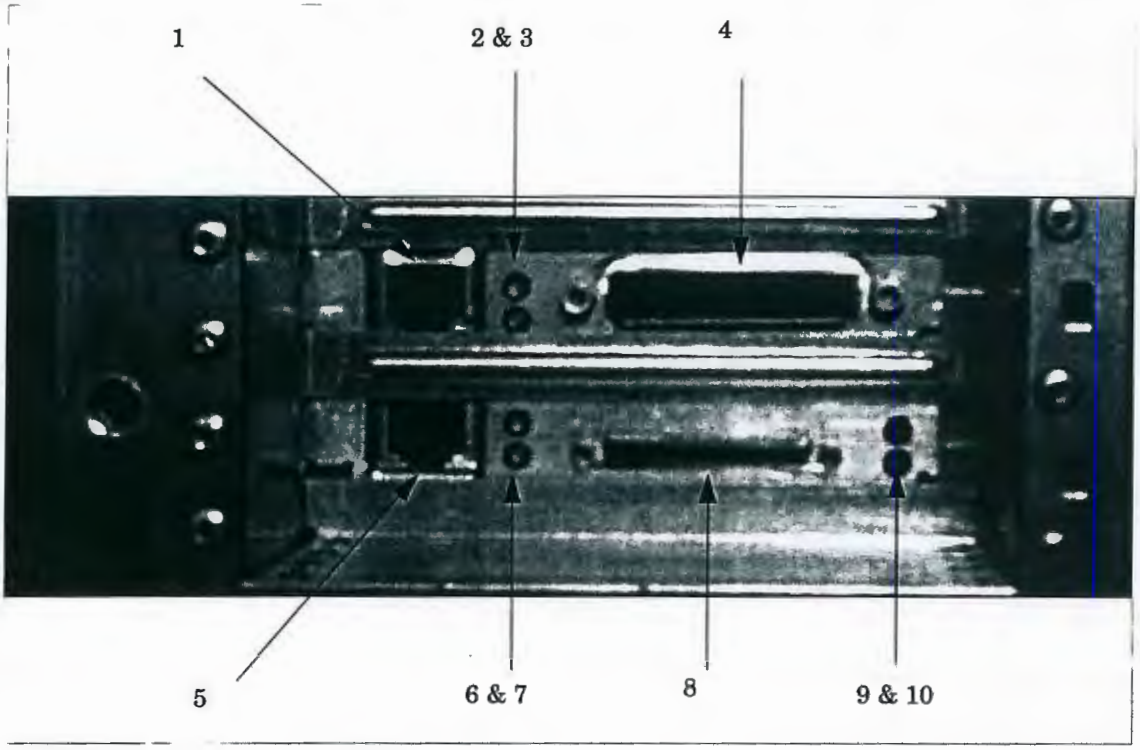


Core I/O Connections

The following paragraphs describe the indicators and connections of the rp54xx Core I/O. Core I/O consists of a LAN/SCSI card in slot 1 (lower slot in graphic) and a Guardian Service Processor (GSP) in slot 2 (upper slot in graphic). There are two versions of GSP, revision A and revision B.

Revision A GSP

The following graphic shows the indicators and connectors for the revision A GSP and LAN/SCSI Core I/O boards.

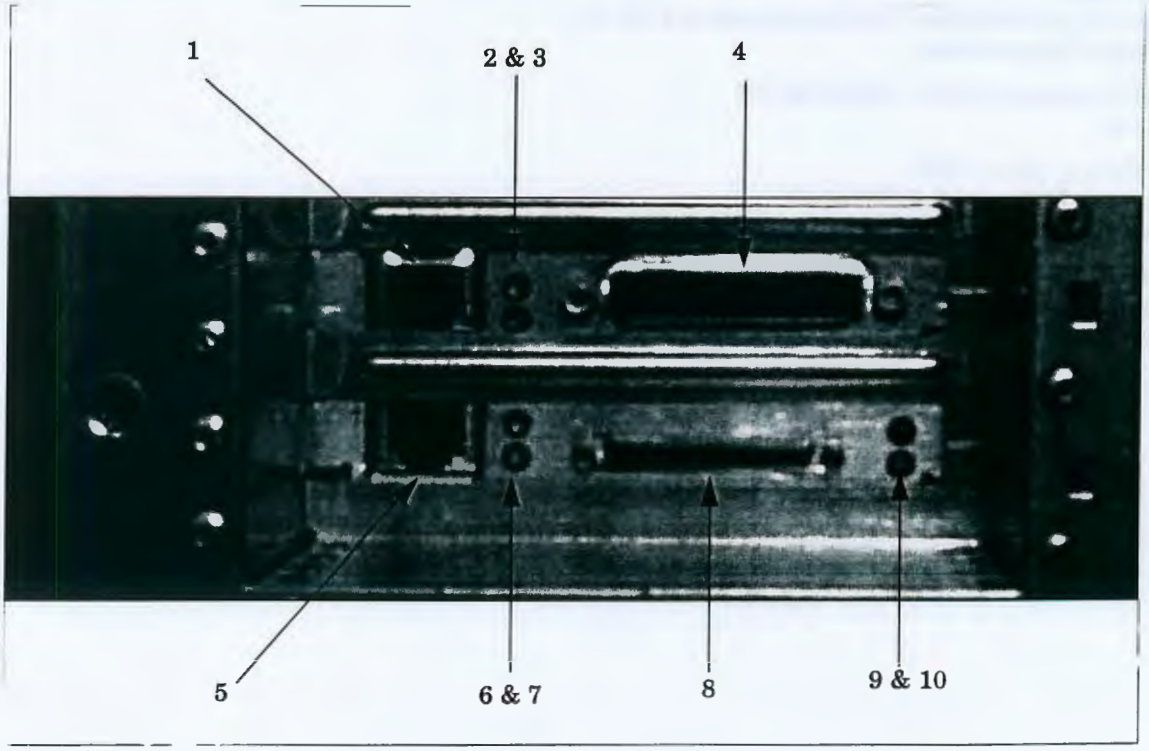


1. 10-Base-T LAN (RJ-45) Connector
   GSP LAN.
2. Green/Red (Upper LED)
   Green = GSP Power On.
   Flashing Green = LAN Receive.
   Red = Guardian Support Processor Test Failed.
3. Green/Red, (Lower LED)
   Green = Link OK.
   Flashing Green = LAN Transmit.
   Red = Guardian Support Processor Test Failed.
4. Console/UPS/Remote Connector (D-Type 25-Pin female).
   Requires an A5191-63001 "W" adapter cable
5. 10/100 Base-T = Primary LAN (RJ-45) Connection
   Path 0/0/0/0

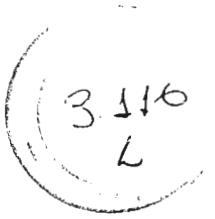
6. Green/Yellow (Upper LED)
   Green = 100 Base-T Mode
   Green Blinking = 100 Base-T Receiving
   Amber = 10 Base-T Mode
   Amber Blinking = 10 Base-T Receiving
7. Green (Lower LED)
   Green = Link OK (10/100 Base-T Mode indicated by LED #6)
   Green Blinking = Transmitting
8. Ultra-2 SCSI Connector (68-Pin VHDCI SCSI)
   Path 0/0/1/0
9. SCSI Mode (Green, Upper LED)
   On = Low Voltage Differential (LVD) Mode.
   Off = Single Ended Mode.
10. SCSI Terminator Power (Amber, Lower LED)
    On = Terminator power present
    Off = Terminator power Not present.

Revision B GSP

The following graphic shows the indicators and connectors for the revision B GSP and LAN/SCSI Core I/O boards.



RQS Nº 03/2005 - CN
CPMI - CORREIOS
0037
Fls:
3701
Doc:



1. 10/100-Base-T LAN (RJ-45) Connector.
   GSP LAN.
2. Green/Red (Upper LED).
   Green = GSP Power On.
   Red = Guardian Support Processor Test Failed.
3. Green/Yellow, (Lower LED).
   Green = 100 Base-T Link OK.
   Flashing Green = 100 Base-T LAN Activity.
   Yellow = 10 Base-T Link OK.
   Flashing Yellow = 10 Base -T LAN Activity.
4. Console/UPS/Remote Connector (D-Type 25-Pin female).
   Requires an A6144-63001 "M" adapter cable.
5. 10/100 Base-T = Primary LAN (RJ-45) Connection.
   Path 0/0/0/0.
6. Green/Yellow (Upper LED).
   Green = 100 Base-T Mode.
   Green Blinking = 100 Base-T Receiving.
   Amber = 10 Base-T Mode.
   Amber Blinking = 10 Base-T Receiving.
7. Green (Lower LED).
   Green = Link OK (10/100 Base-T Mode indicated by LED #6).
   Green Blinking = Transmitting.
8. Ultra-2 SCSI Connector (68-Pin VHDCI SCSI).
   Path 0/0/1/0.
9. SCSI Mode (Green, Upper LED)
   On = Low Voltage Differential (LVD) Mode.
   Off = Single Ended Mode.
10. SCSI Terminator Power (Amber, Lower LED)
    On = Terminator power present
    Off = Terminator power Not present.

Guardian Service Processor (GSP) Overview

This section provides an overview of the Guardian Service Processor (GSP). The GSP is an always on, dedicated service processor that monitors system power, cooling and configuration, and provides console communications. Power and cooling information is obtained via an interface to the platform monitor card. Configuration information is obtained via connection to the Serial Presence Detect (SPD) bus. The GSP can only be installed in slot 2 and must be present for the server to power up.

The GSP has downloadable firmware which can be updated independent of the HP-UX operating system. GSP firmware updates can occur anytime the GSP is active. If the DC power switch is OFF, the GSP is still operational and GSP firmware updates can still occur. GSP firmware updates may be performed by customers.

If the GSP becomes hung, it is possible to reset the GSP without impacting the server. The GSP may be reset via the GSP RESET button on the right side of the card. The PCI cover panel (right side panel) must first be removed to allow access to the right side if the GSP card.

The GSP has two connectors on the bulkhead. An RJ-45 for LAN connections and a female DB25 connector for RS-232 connections. Attach either a "W" or an "M" cable to the DB25 connector to provide individual output or CONSOLE, REMOTE and UPS.

To access the GSP from the local ASCII console, type control b and the GSP> prompt will appear. It may be necessary to type control Ecf first. To exit the GSP, type GSP>co.

The GSP was originally a core component of the revision A rp5400 (A5576A) and rp5450 (A5191A) servers. Beginning with introduction of the revision B rp5400 (A5576B), rp5450 (A5191B), and rp5470 servers the GSP became a separate, must order product (A6696A).

There are two revisions of rp54xx GSP: rev A (A6696A) and rev B (A6696B). Both GSPs must be installed in order for the server to power up.

GSP LAN

This LAN is exclusively for LAN console access and is not configurable via HP-UX. The LAN is configured via GSP commands. Hostname, IP, gateway and subnet mask parameters may be set via the GSP>lc command. The GSP may also initiate ping via the GSP>xd command.

GSP RS-232

The DB25 connector on the GSP is used for RS-232 communications to a local console (via CONSOLE connector), a remote console via modem (REMOTE connector), and a UPS (UPS connector). The baud rate, term type, etc., of the CONSOLE and REMOTE ports are configured via GSP>ca command.

The GSP supports VT100 and HPTERM terminal emulation. For correct communications, the GSP and RS-232 device must use the same terminal emulation and baud rates.

GSP Features

The revision A GSP provides a 10 base-T LAN connector for LAN console access and a DB-25 connector to which the A5191-63001 W-cable connects. The W-cable provides REMOTE, UPS, and CONSOLE DB-9 connectors.

Features of the revision A GSP are:

- 10 Base-T LAN connector for revision A GSP

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0038
Fls:
Doc: 3791

- 10/100 Base-T LAN connector for revision B GSP
- On-board processor dedicated to GSP functions
- Error logging and notification
- Display of system alerts and selftest chassis codes
- Powered by 15 VDC housekeeping power that is present when the front panel switch is off
- Power and configuration monitoring
- RS-232, LAN, REMOTE and WEB console access
- Administrator and user security
- Alphanumeric paging.

There are two revisions of rp54xx GSP: revision A (A6696A) and revision B (A6696B). Due to significant hardware differences between the revision A and B GSP, each GSP requires it's own firmware. Revision A GSP firmware can only be installed in a revision A GSP and revision B GSP firmware can only be installed in a revision B GSP. The hardware differences are necessary to incorporate the embedded web access, 10/100 Base-t LAN, and faster GSP processor.

The GSP provides four types of console access: RS-232, Remote, LAN and Web. Console information is mirrored to all four console types. Refer to *Configure System Console* for more information.

The GSP was originally a core component of the revision A rp5400 (A5576A) and rp5450 (A5191A) servers. Beginning with introduction of the revision B rp5400 (A5576B), rp5450 (A5191B), and rp5470 servers the GSP became a separate, must order product (A6696A).

Revision A GSP

The revision A GSP is identified by product number A6696A and part numbers: A5191-60012, A5191-69012, and A5191-69112.

The revision A GSP requires a "W" cable to be attached to the DB25 connector. The part number of the "W" is A5191-63001. The "W" cable provides female DB9 connectors for CONSOLE, REMOTE and UPS. The maximum supported baud rate for the CONSOLE and REMOTE connectors is 19200 baud and 1200 baud for the UPS.

The paths for the CONSOLE, UPS, and REMOTE are 0/0/4/0.0, 0/0/4/0.1, and 0/0/4/0.2 respectively.

For the rev A GSP, the web console is accomplished by shipping one J3591A Secure Web Console with each rp54xx server. The Secure Web Console can be used in place of an ASCII console to provide console access via a web connection. If you are installing an rp54xx server that does not have an ASCII console, you may use the Secure Web Console as the console. However, you must first configure the Secure Web Console. Refer to *Secure Web Console Installation and Configuration* for more information on SWC Installation/Configuration.

Revision B GSP

The revision B GSP is identified by product number A6696B and part numbers: A6144-60012, A6144-69012, and A6144-69112.

The revision B GSP requires an "M" cable to be attached to the DB25 connector. The part number of the "M" cable is A6144-63001. The "M" cable provides female DB9 connectors for CONSOLE, REMOTE, and UPS. The maximum supported baud rate for the CONSOLE and REMOTE connectors is 38400 baud and 1200 baud for the UPS.

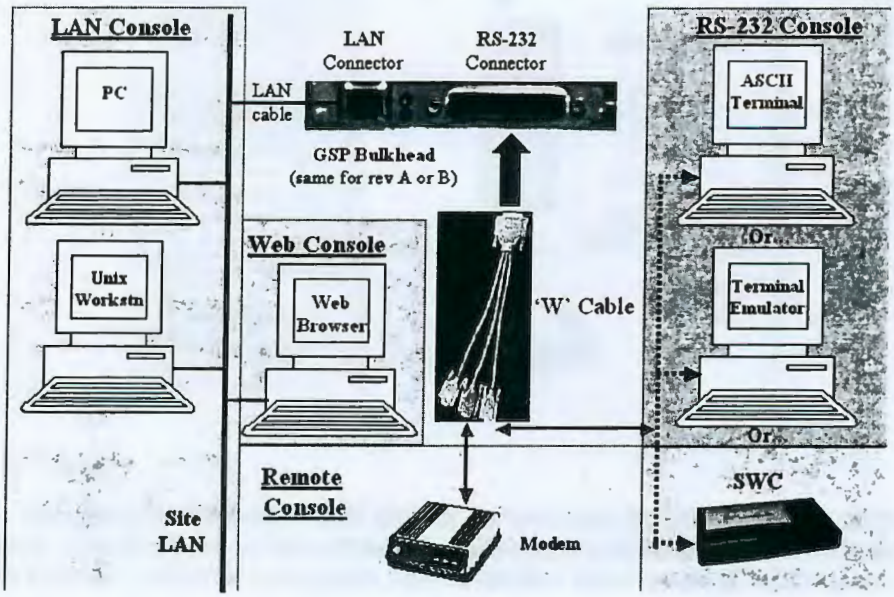
The paths for the CONSOLE, UPS, and REMOTE are 0/0/4/1.0, 0/0/4/1.1 and 0/0/4/1.2 respectively.

ECT 3.113 June

Configure System Consoles

rp54xx servers provide RS-232, REMOTE, LAN and WEB console access. All console access involves the Guardian Service Processor (GSP). rp54xx servers use either a revision A or revision B GSP. Below is an illustration of the console access provided by the revision A GSP.

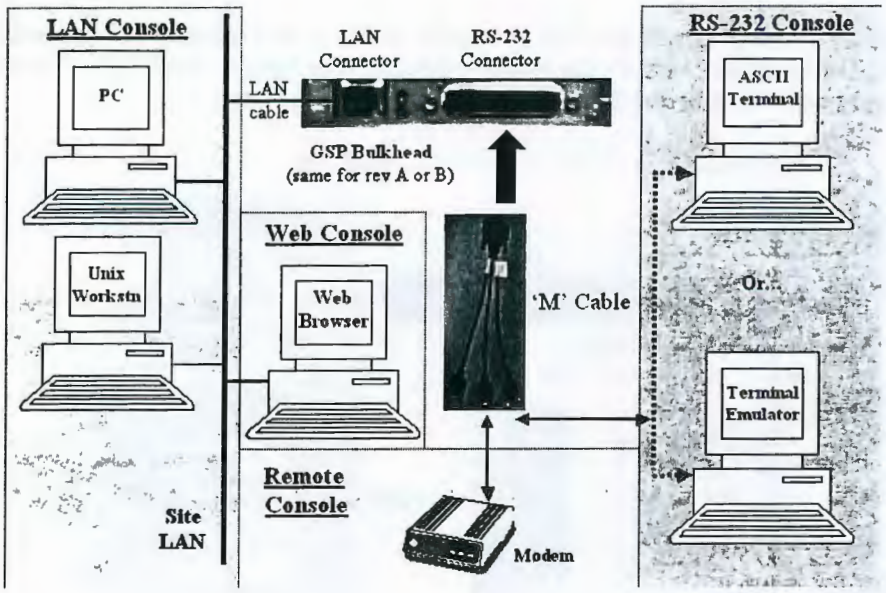
Revision A GSP Console Access



The revision B GSP has embedded web access, eliminating the need for an external Secure Web Console (SWC). Below is an illustration of the console access provided by the revision A GSP.

IRQS Nº 03/2005 - CN
CPMI - CORREIOS
0039
Fls:
3701
Doc:

Revision B GSP Console Access



GSP Cables

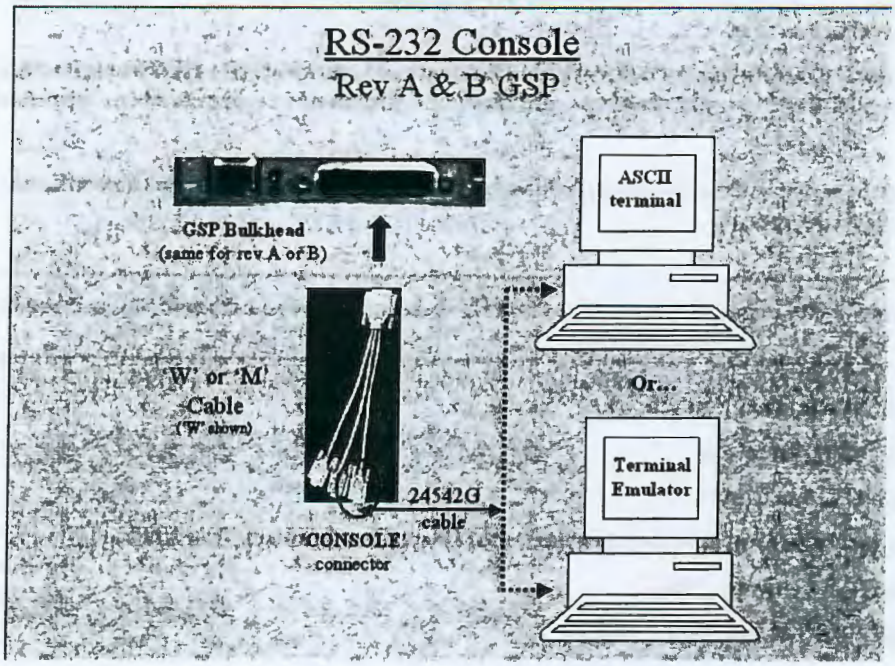
Both the revision A and B GSPs provide a DB-25 connector for RS-232 communications. Connect the A5191-63001 W- cable to the revision A GSP DB25 connector or connect the A6144-63001 M-cable to the revision B GSP DB25 connector. These cables provide individual DB9 connectors for REMOTE, UPS and CONSOLE.

NOTE Use the A5191-63001 W-cable with revision A GSP and A6144-63001 M-cable with revision B GSP *only*. Failure to use the right cable can result in reduced functionality.

The W and M-cables are slightly different. The W-cable has full RS-232 capability on the REMOTE and CONSOLE connectors and partial RS-232 capability on the UPS connector. The M-cable has full RS-232 capability on the REMOTE and UPS connectors and partial RS-232 capability on the CONSOLE connector. The cable change is to be consistent with rp54xx functionality. The cables are different colors to easily tell them apart. The W-cable is gray and has part number A5191-63001. The M-cable is black and has part number A6144-63001.

Configure RS-232 Console

The physical connections for an RS-232 console include attaching the correct cable to the GSP. Next, connect the 24542G cable (supplied) to the CONSOLE connector and the serial port of the ASCII console. A personal computer (PC) running terminal emulation software may be used in place of an ASCII console. Refer to the illustration below for RS-232 console.



Step 1. The GSP is located in slot 2 of the rp54xx' rear card cage. Connect the 25-pin end of:

- the A5191-63001 W-cable to the 25-pin connector on the revision A GSP card (A5191-60012) OR
- the A6144-63001 M-cable to the 25-pin connector on the revision B GSP card (A6144-60012)

Step 2. Connect the 9-pin "Console" connector of either the W or M-cable to the 9-pin D-type connector of a 24542G RS-232 cable.

Step 3. Connect the 25-pin end of the 24542G serial cable to the serial/RS232 port on the ASCII console. (RS232 Serial Port labeling may vary depending on manufacturer.)

Step 4. Connect the System Console to input AC power.

Step 5. Turn the System Console AC power switch to ON.

After the physical connections have been made, configure the ASCII console. When using the C1099A Terminal Console, the default settings are recommended. Refer to the C1099A Terminal Console operating manual for instructions on how to obtain default settings.

The HP 700 series console may also be used as an ASCII console. Both the C1099A Terminal Console and S700 consoles support HPterm and VT100 emulations. The emulation of the GSP and ASCII console need not match for communications between them to occur. However, to ensure proper communications, HP recommends the ASCII console and GSP use the same emulation. HP also recommends that other configurable parameters on the GSP match those of the ASCII console. Baud rate, start/stop bits, etc... The default emulation of the GSP is VT100.

Below is a procedure to configure a HP 700 serial console for VT100 emulation.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 0040
Doc: 3701

HP 700 Series System Console Configuration

The following describes the steps required to configure the HP 700 series terminal for VT-100 mode for operation with an rp54xx server.

Although any terminal capable of operating in VT-100 mode can be used, the HP700 series terminal is used here as an example because it is fairly common and it's configuration is typical of many terminals currently in use.

HP700 VT-100 Mode Configuration The following procedure outlines the steps to configure the HP700 series terminal for VT100 operation.

NOTE You may use either the arrow keys or the tab key to move between the setting options on the screen.

---

1. Press **[config keys]** function key. **[f8]**
2. Press **[terminal config]** function key. **[f5]**
3. Move to *Terminal ID* and enter "vt100".
4. Move to *Set TermMode* and, using the **[Prev]** and **[Next]** keys, select "EM100".
5. Press the **[config keys]** function key. **[f8]**
6. Press the **[ansi config]** function key. **[f6]**
7. Move to "multipage" and, using the **[Prev]** and **[Next]** keys, select "yes". (Enables screen scrolling).
8. Move to *Backspace Del* and, using the **[Prev]** and **[Next]** keys, select "Backspace/Del".
9. Move to *EM100 ID* and, using the **[Prev]** and **[Next]** keys, select "EM100".

Configure the Asynchronous Values of the GSP

After the ASCII console has been configured and physical connections made, make any necessary changes to the asynchronous values of the GSP.

1. Access the GSP with the ctrl+b entry. The GSP will respond with a GSP> prompt.
2. At the GSP prompt, enter the Configure Asynchronous (ca) command:

The ca command will start a series of prompts. Respond to each prompt with the appropriate information.

Example 4-1 CA command

```
Leaving Console Mode - you may lose write access. When Console Mode returns, type
^Ecf to get console write access.

GSP Host Name:  fesrhapgsp

GSP> ca

CA This command allows you to modify the local and remote modem serial
portconfigurations.

Current configuration settings:

Local Console Serial Port bit rate: 9600 bits/s

Local Console Serial Port Flow Control: Software
```

3.109
Irene


```
Local Console Serial Port Terminal Type: vt100
Remote Console Serial Port Modem Protocol: CCITT  Remote Console Serial Port Modem
bit rate: 19200 bits/s
Remote Console Serial Port Modem Flow Control: Software
Remote Console Serial Port Modem Transmit Configuration Strings: Enabled
Remote Console Serial Port Modem Presence: always connected
Do you want to modify the Local Console Serial Port settings? (Y/[N])
Do you want to modify the Remote Console Serial Port Modem settings? (Y/[N])
GSP Host Name:  fesrhapgsp
```

If necessary, use the GSP help facility by typing GSP>he. Once in the help facility, type the command need help with. Use LI for a list of commands.

The following baud rates are recommended for the revision A GSP:

- Console: 19200
- Remote: 19200
- UPS: 1200

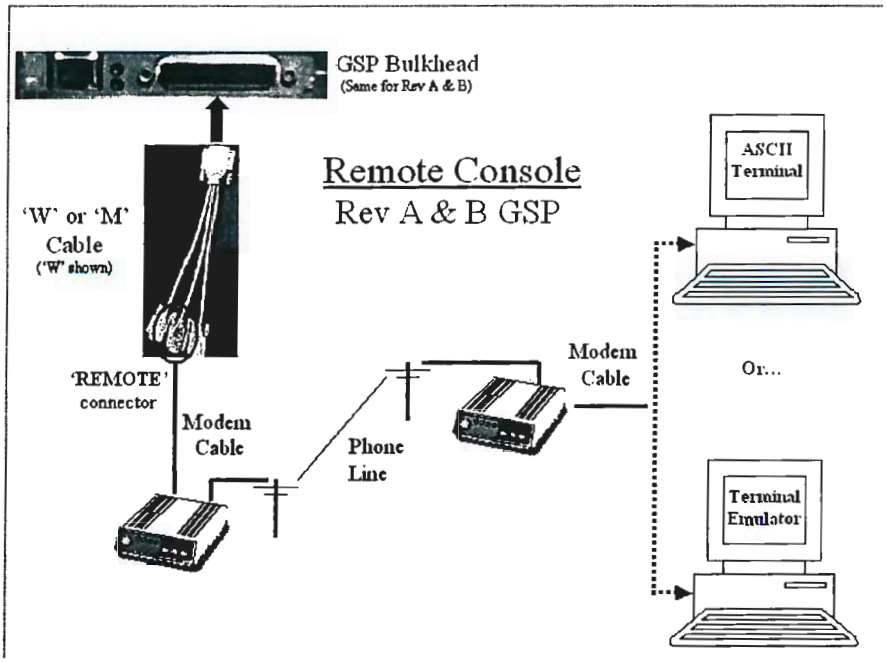
The following baud rates are recommended for the revision B GSP:

- Console: 38400
- Remote: 38400
- UPS: 1200

RQS Nº 03/2005 - CN
CPML- CORREIOS
0041
Fls:
Doc:

Configure Remote Console

The remote console allows console access via modem connections. Below is an illustration of the REMOTE console.

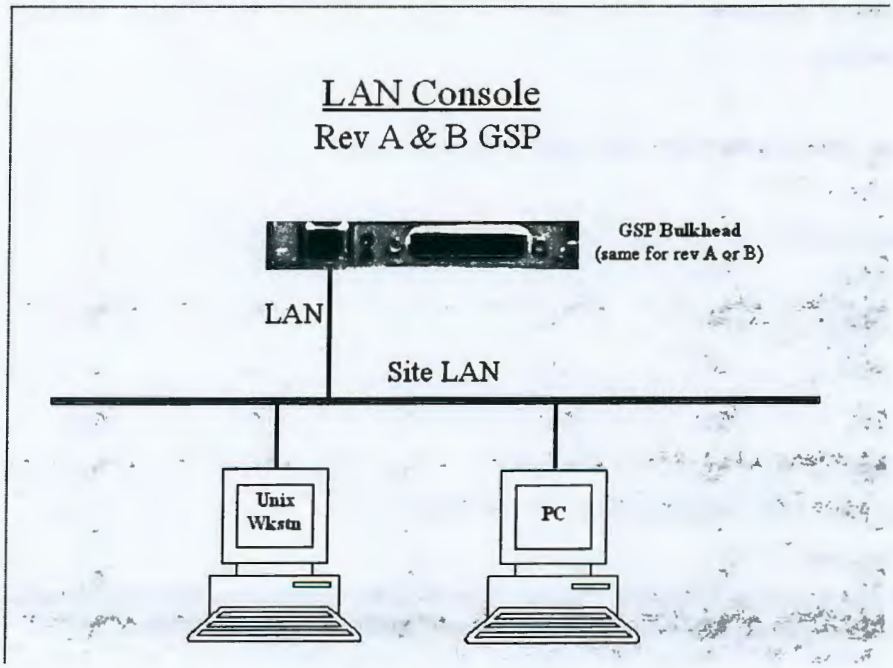


The GSP>ca command is used to configure asynchronous settings for the REMOTE console. Baud rates and emulations should match between the modems, remote ASCII terminal and the GSP. Refer to, "Configure RS232 Console" for information about setting these values.

3.107
frente
CPI - AC

Configure the LAN Console

The LAN console allows you to access the console from the LAN using TelNet or http (revision B GSP only) protocols. Below is an illustration of the LAN console.



The configuration of the LAN console of both the revision A and B GSPs may be done from either an ASCII console or the external Secure Web Console. For the revision B GSP, an IP may be assigned via LAN by pinging the LAN from a PC or workstation.

Configuring the GSP LAN Port via an ASCII console

The LAN port of the GSP allows connection via TelNet or http connections. Once the LAN parameters are configured, the console may be accessed via a TelNet connection or via a web browser (revision B GSP only). The default IP of the GSP LAN is 127.0.0.1.

NOTE The GSP has a separate LAN port from the system LAN port. It will need a separate LAN drop, IP address, and networking information from the port used by HP-UX.
Before starting this procedure, you will need to know the following information:

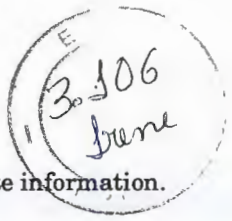
- I.P. address (for GSP)
- Subnet mask
- Gateway address
- Hostname (this is used when messages are logged or printed)

To configure the GSP LAN port, perform the following steps:

1. Access the GSP with the ctrl+b entry.
2. At the GSP prompt, enter the LAN Configuration (lc) command:

```
GSP> lc
```


ROS Nº 03/2005 - CN
CPMI - CORREIOS
0042
Fls:
3701
Doc:



The lc command will start a series of prompts. Respond to each prompt with the appropriate information.

Example 4-2 LC command

```
Leaving Console Mode - you may lose write access. When Console Mode returns, type
^Ecf to get console write access.

GSP Host Name:  fesrhapgsp

GSP> lc

LC This command allows you to modify the LAN configuration.

Current configuration:

MAC Address: 0x00306e050a63

IP Address: 15.8.133.185

GSP Host Name: fesrhapgsp

Subnet Mask: 255.255.248.0

Gateway: 15.8.128.1

Web Console Port Number: 2023

Do you want to modify the LAN configuration? (Y/[N])

GSP Host Name:  fesrhapgsp
```

The revision B GSP introduces a configurable Web Console Port Number parameter. The default value is 2023. Once the GSP LAN is configured, it is accessible via either TelNet or web connections.

Configuring the GSP LAN Port via LAN

The revision B GSP LAN port can be assigned an IP address without using the LAN Configuration (lc) command via an ASCII console. This section describes how to assign the IP address allowing web access. Once web access is accomplished, use the lc command to configure remaining network parameters.

NOTE The GSP LAN port is separate from the system LAN port. It will need a separate LAN drop, IP address, and networking information from the port used by HP-UX.
Before starting this procedure, you will need to know the following information:

- I.P. address (for GSP)
- Subnet mask
- Gateway address
- Hostname (this is used when messages are logged or printed)

To configure the GSP LAN port via LAN, perform the following steps:

NOTE The GSP *must* be on the same subnet as the system being used to remotely configure the LAN port. If it is not, the remote configuration will be unsuccessful.

Step 6. Determine the MAC address of the revision B GSP by examining the GSP MAC address label on the rear of the server.

Step 7. Use the `route add` command to add the I.P address of the GSP and remote system to the router.

3.105 fume

Step 8. Use the arp command to add an ARP entry for the IP address using the GSP MAC address.

- For HP-UX systems, the format of the MAC address is 00:30:6e:05:0a:ea
- For MS DOS systems, the format of the MAC address is 00-30-6e-05-0a-ea

Step 9. Use the ping command to assign the I.P address for the GSP.

Step 10. The revision B GSP is now accessible via LAN. Access the GSP and configure remaining network parameters using the LAN Configuration (lc) command:

```
GSP> lc
```

The lc command will start a series of prompts. Respond to each prompt with the appropriate information.

Example 4-3 LAN Configuration from a PC

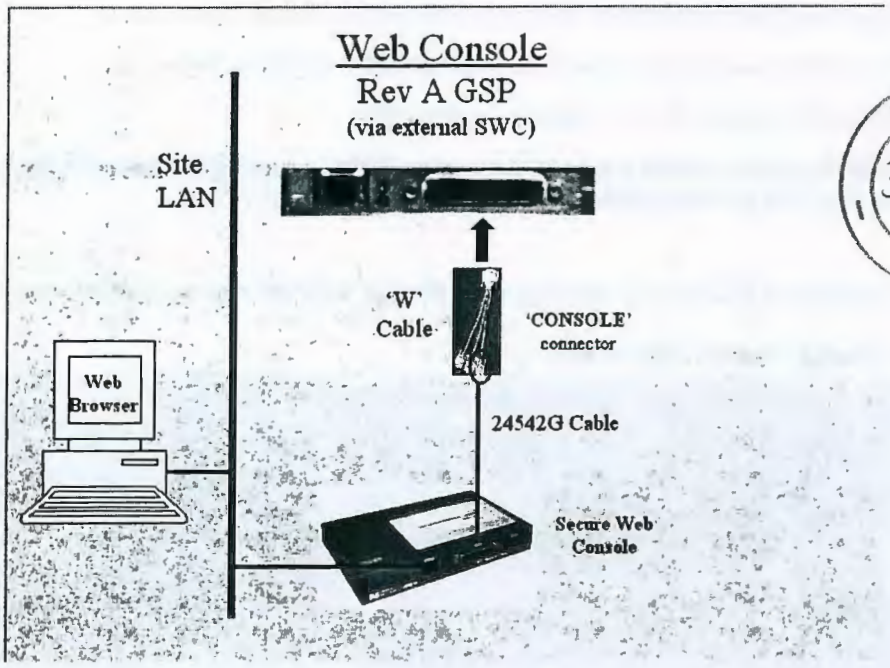
```
Command Prompt
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-1999 Microsoft Corp.

C:\>route add 15.8.130.1 15.8.133.147

C:\>arp -s 15.8.130.1 00-30-6e-05-0a-ea

C:\>ping 15.8.130.1

Pinging 15.8.130.1 with 32 bytes of data:

Reply from 15.8.130.1: bytes=32 time<10ms TTL=63
Reply from 15.8.130.1: bytes=32 time<10ms TTL=63
Reply from 15.8.130.1: bytes=32 time<10ms TTL=63
Reply from 15.8.130.1: bytes=32 time<10ms TTL=63

Ping statistics for 15.8.130.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum =  0ms, Average =  0ms

C:\>
```

Configure the Web Console

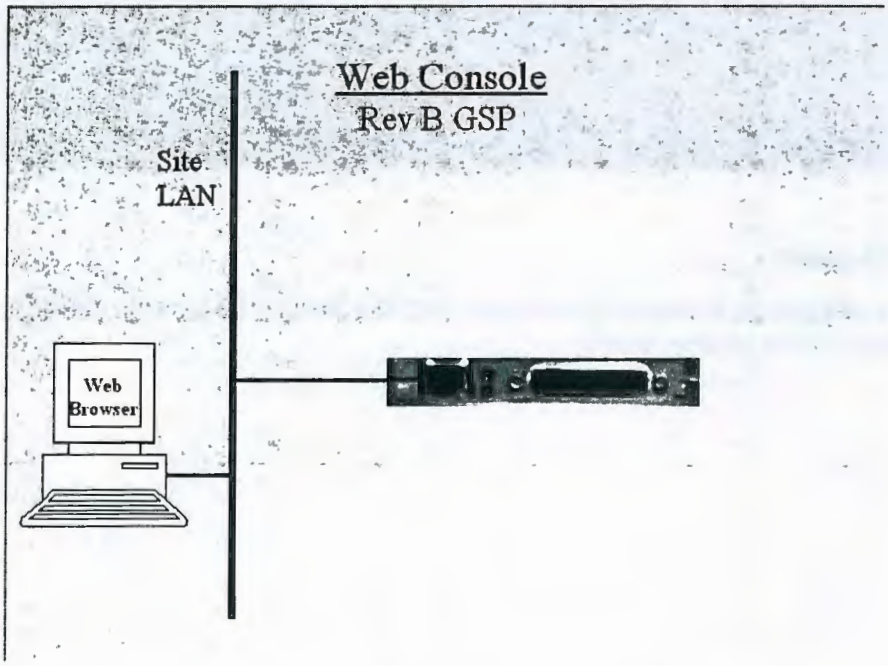
For the revision A GSP, the web console is accomplished via the J3591A Secure Web Console. Below is an illustration of the web console for the revision A GSP.

ROS Nº 03/2005 - CN
CPMI - CORREIOS
0043
Fls:
3701
Doc:

Refer to, "Install a Secure Web Console" for more information on Secure Web Console installation and configuration.



For the revision B GSP, the web console is an embedded feature. The steps to configure a web console are the same as configuring a LAN console. Refer to, "Configure the LAN Console."



Once the LAN has been configured, access the web console by pointing a web browser, on the same subnet, to the IP of the GSP LAN.

3.004 Itens

Processor Support Module Removal

Processor Support Modules (PSMs) reside on the System Board and are accessed via the Top Service Bay. Looking into the Top Service Bay from the front, PSMs are located on either side of the server, at the front. There can be two PSMs, numbered 0 and 1

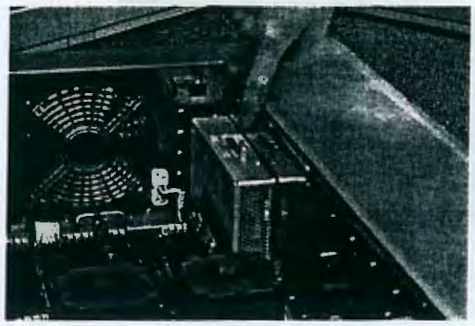
To remove a PSM from the server, perform the following steps:

1. Loosen the two captive mounting screws that hold the PSM in place.

NOTE For the rp5470, the mounting screws have been replaced by posts and the air baffle is used to secure the PSM's.

2. Grasp the two captive mounting screws and lift the PSM out of the server.

The following graphic shows a PSM in the server.



ROSN 05/2005 GN
CPMI - CORREIOS
Fls: 0044
Doc: 3701

HotSwap Power Converter Fan Replacement

The power to the server does not have to be off to remove or replace a HotSwap Power Converter fan. Fans numbered 6 and 7 are located in the rear of the server.

To replace a fan into the server, perform the following steps:

1. Orient the fan assembly so that the electrical plug will connect, then grasp the extended screw-heads (or the fan grill) and gently push the fan assembly into its housing. The fan assembly plug will connect with the electrical outlet in back of the housing.
2. Tighten the captive T-15 screws located diagonally across the face of the fan (upper left, lower right sides).

The following graphic shows where HotSwap Power Converter Fans are located.

3.006

HotSwap Power Converter Fan Removal

The power to the server does not have to be off to remove or replace a HotSwap Power Converter fan. Fans numbered 6 and 7 are located in the rear of the server.

To remove a fan from the server, perform the following steps:

NOTE When one fan has failed (or is removed from the server), the system automatically puts the remaining fan into high speed mode. The noise level of the server will increase.

1. There are four screws attached to each corner of each fan. Loosen only the captive Torx-head screws located diagonally across the face of the fan (upper left, lower right sides).
2. Grasp the extended screw-heads (or the fan grill) and gently pull toward you. The fan assembly will unplug from the electrical outlet and slide out of the server.

CAUTION Running the server for extended periods of time with a cooling fan removed may create hot spots inside the server and possibly shorten component life.

If the other fan fails when one fan is removed, the system will halt.

The following graphic shows where HotSwap Power Converter Fans are located.

ROS Nº 0372005 - CN
CPMI - CORREIOS
0045
Fls:
Doc: 3791

HotSwap Power Supply Replacement

Up to three power supplies (0 through 2), located across the bottom front of the server, can be installed in the server without removing power.

To replace a power supply, perform the following steps:

CAUTION Be careful when putting the power supply into the server. It is heavier than it appears.

1. Grasp the handle in one hand and support the power supply with the other. Slide the power supply into the server. The Power Supply LED should illuminate immediately.
2. Replace the T-15 mounting screw located to the right of the handle near the top of the power supply.

The following graphic shows a front and rear view of a HotSwap Power Supply.

ECT 3.008 frente

HotSwap Power Supply Removal

Up to three power supplies (0 through 2), located across the bottom front of the server, can be installed in the server without removing power.

To remove a power supply from the server, perform the following step:

1. Remove the T-15 mounting screw located to the right of the handle near the top of the power supply.

CAUTION Be careful when pulling the power supply out of the server. It is heavier than it appears.

2. Grasp the handle and pull the power supply out of the server.

The following graphic shows a front and rear view of a HotSwap Power Supply.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 0046
Doc: 3701

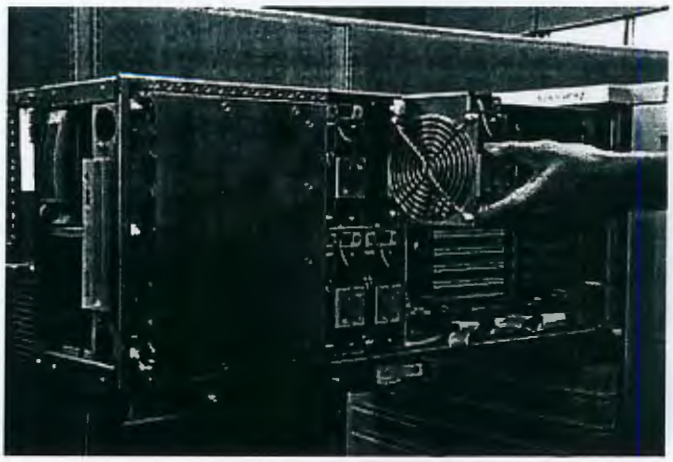
3.009 Irene CPI-AS

HotSwap Card Cage Fan Replacement

The power to the server does not have to be off to remove or replace a HotSwap Card Cage fan. Fans numbered 2, 3, 4, and 5 are located in a four-fan assembly housing located on the left side of the server's side service bay.

To replace a fan in the server, orient the replacement fan into its slot in the Side Fan Assembly Housing and carefully push it in until it connects with its electrical outlet on the I/O Backplane.

The following graphic shows a card cage fan being removed/replaced.



3.010 fls 1
CPL - AC

HotSwap Card Cage Fan Removal

The power to the server does not have to be off to remove or replace a HotSwap Card Cage fan. Fans numbered 2, 3, 4, and 5 are located in a four-fan assembly housing located on the left side of the server's side service bay.

CAUTION Running the server for extended periods of time with a cooling fan removed may create hot spots inside the server and shorten component life.

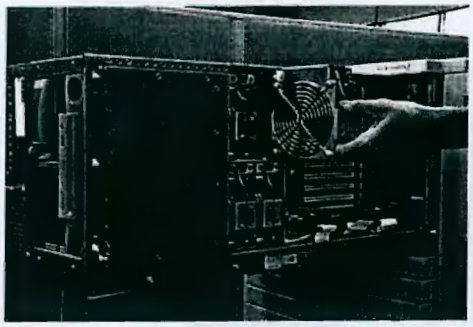
If other fans fail when one fan is removed, the system will halt.

To remove a fan from the server, perform the following step:

Identify the fan to be removed and pull it out of the Side Fan Assembly Housing. It will automatically disconnect from its electrical outlet on the I/O Backplane.

NOTE When one fan has failed (or is removed from the server) during operation, the system automatically puts the remaining fans into high speed mode. The noise level of the server will increase.

The following graphic shows a card cage fan being removed/replaced.



RQS Nº 03/2005 - CN
CPMI - CORREIOS
0047
Fls:
Doc: 3701

HotSwap Chassis Fan Replacement

The power to the server does not have to be off to remove or replace a HotSwap Chassis fan. Fan number 0 is located in the front of the server and fan number 1 is located at the rear of the server.

To replace a fan, perform the following steps:

1. Orient the fan assembly to ensure that the chassis outlet connects with the fan assembly. If the fan power connector is covered by the protective cover (see item 1 in the graphic), slide it down to remove it and slide it over the power connection on the other side of the fan. Push the fan firmly into the housing. The fan assembly will plug into the electrical outlet automatically.
2. Check the LED located on the fan.
   - When the fan is functioning normally, the LED is OFF.
   - When the fan fails, the LED is ON.

NOTE when one fan has failed (or is removed from the server), the system automatically puts the remaining fan into high speed mode. The noise level of the server will increase.

3. Replace the HotSwap Chassis fan cover.

The following graphic shows a HotSwap Chassis Fan.

E C T
3012
Fls.
C P L - A C

HotSwap Chassis Fan Removal

The power to the server does not have to be off to remove or replace a HotSwap Chassis fan. Fan number 0 is in the front of the server and fan number 1 is at the rear of the server.

To remove a fan from the server, perform the following steps:

1. Check the fan LED located on the fan. If the LED is illuminated, the fan has failed.

NOTE When one fan has failed (or is removed from the server), the system automatically puts the remaining fan into high speed mode. The noise level of the server will increase.

---

2. Grasp the fan grill and gently pull toward you. The fan assembly will unplug from the electrical outlet and slide out of the server.

CAUTION Running the server for extended periods of time with a cooling fan removed may create hot spots inside the server and possibly shorten component life.

If the other fan fails when one fan is removed, the system will halt.

The following graphic shows a HotSwap Chassis Fan.

CPMI - 03/2005 - CN
CPMI - CORREIOS
0048
Fls:
Doc: 2701

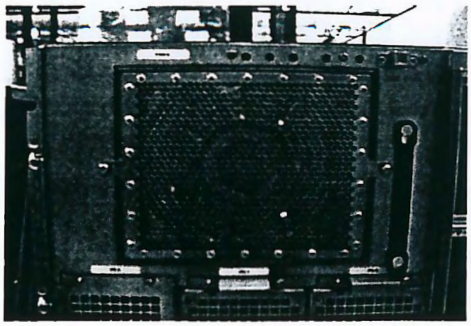
HotSwap Chassis Fan Cover Replacement

The power to the server does not have to be off to remove or replace a HotSwap Chassis Fan cover. Fan number 0 is located in the front of the server and fan number 1 is located at the rear of the server.

To replace a chassis fan cover, perform the following tasks:

1. Insert the cover into position in front of the fan.
2. Tighten the captive T-15 screws on each side of the cover.

The following graphic shows a HotSwap Chassis Fan Cover.



3014
fls

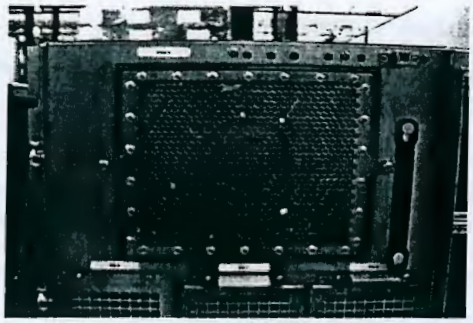
HotSwap Chassis Fan Cover Removal

Power to the server does not have to be off to remove or replace a HotSwap Chassis fan cover. Fan number 0 is in the front of the server and fan number 1 is at the rear of the server.

To remove a fan cover from the server, perform the following steps:

1. Loosen the captive T-15 screws from the sides of the cover.
2. Gently pry the cover away from the server and set it aside.

The following graphic shows a Chassis Fan Cover in place.



RQS Nº 03/2005 - CN
CPMI - CORREIOS
0049
Fls:
3701
Doc:

g. Verify that the mirroring is set up properly.

For example:

```
# vgdisplay -v /dev/vg00
# lvdisplay /dev/vg00/lol1 - lvol8
# lvlnboot -v /dev/vg00
```

Both disks should list as "Boot Disk" and both should appear in the *lvol* lists.

At this point the system will be fully functional.

Hot Swap Procedure for Unattached Physical Volumes

The following steps are an example of how to replace a HotPlug disk drive for unattached physical volumes. This example assumes the disks are mirrored.

NOTE HP often uses different manufacturers for disks, but assigns the same product number. The hot swap manual procedure will not update disk driver internal information to that of the replaced disk drive.

Step 1. Perform an *ioscan* on the replaced disk drive to ensure that it is accessible (claimed), to double check that it is a proper replacement, and that the device files are present. Refer to the above note.

For example: `# ioscan -fnC disk`

Step 2. Restore the LVM configuration/headers onto the replaced disk drive from your backup of the LVM configuration with the following entry:

```
# vgcfgrestore -n <volume group name> /dev/rdsk/cXtXdX
```

For example: `# vgcfgrestore -n /dev/vg00 /dev/rdsk/cXtXdX`

Step 3. Attach the new disk drive to the active volume group with the following *vgchange* command:

```
# vgchange -A y <volume group name>
```

For example: `# vgchange -A y /dev/vg00`

Step 4. Use the *mkboot* command to make the device bootable.

For example: `# mkboot /dev/rdsk/cXtXdX`

Step 5. Use the *mkboot* command again to add the HP-UX auto-file-string.For example: `# mkboot -a "hpux" /dev/rdsk/cXtXdX`

Step 6. Run *lvlnboot* with the following command: `# lvlnboot -R`

Step 7. Resynchronize the mirrors of the replaced disk drive with the following command. It may take several minutes to copy all the data from the original copy of the data to the mirrored extents. The logical volume(s) are still accessible to users' applications during this command.

```
# vgsync <VG name>
```

For example: `# vgsync /dev/vg00`

At this point the system will be fully functional.

3.016 June

Hot Swap Software Procedure for Attached Physical Volumes

The following procedure is an example of how to recover from replacing a disk that was recognized as an attached physical volume. Be sure that all the software procedures in the *Disk Drive Removal* section have been completed prior to starting these steps. This example assumes that the disk was mirrored.

NOTE HP often uses different manufacturers for disks, but assigns the same product number. The hot swap manual procedure will not update disk driver internal information to that of the replaced disk drive.

Step 1. Perform an *ioscan* on the replaced disk drive to ensure that it is accessible (claimed), to double check that it is a proper replacement, and that the device files are present. Refer to the above note.

For example: `# ioscan -fnC disk`

Step 2. Use the following procedure to mirror the root disk:

a. Create the new physical volume using the *pvcreate* command.
For example: `# pvcreate -B /dev/rdsk/cXtXdX`

b. Extend the volume group to include the new physical volume using the *vgextend* command:
For example: `# vgextend /dev/vg00 /dev/dsk/cXtXdX`

c. The *mkboot* command must be run to make the device bootable.
For example:`# mkboot /dev/rdsk/cXtXdX`

d. Use the *mkboot* command again to add the HP-UX auto-file-string.
For example: `# mkboot -a "hpux" /dev/rdsk/cXtXdX`

e. Run *lvlnboot* with the following command: `# lvlnboot -R`

f. Run *lvextend* to put a mirror into the replaced disk drive. It may take several minutes to copy the original copy of the data to the mirrored extents. The logical volume(s) will still be accessible to user applications during this operation.

For example:
```
# lvextend -m 1 <LV name> /dev/dsk/cXtXdX
OR
# lvextend -m 2 <LV name> /dev/dsk/cXtXdX (for 3 way mirroring)
```

For example:
```
# lvextend -m 1 /dev/vg00/lvol4 /dev/dsk/cXtXdX
OR
# lvextend -m 1 /dev/vg00/lvol5 /dev/dsk/cXtXdX
```

Repeat this for each logical volume to be mirrored.

Verify that the mirror is bootable and AUTO file is correct.

```
For example:
# lifls -l /dev/rdsk/cXtXdX
OR
# lifcp /dev/rdsk/cXtXdX:AUTO -
```


RQS Nº 03/2005 - CN - Chapter 2005 - CN
CPMI - CORREIOS
Fls: 0050
Doc: 3701

HotPlug Disk Drive Replacement

The internal disk drives (up to four) are located at the front right side of the server (as you are facing it). When proper software and hardware procedures are followed, internal disk drives can be removed and replaced while the server is running.

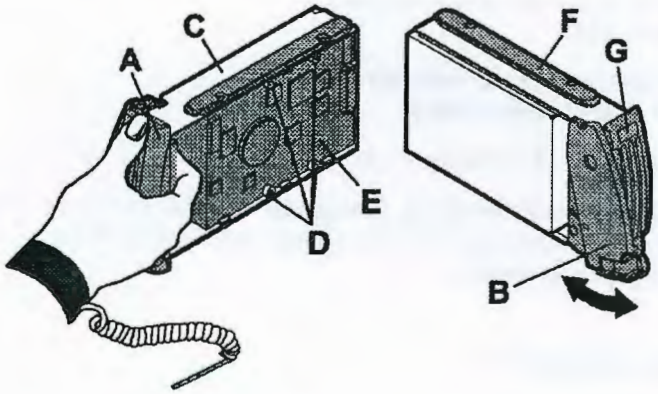
CAUTION Disk Drives can be removed or installed with the server still powered on. This is referred to as a "manual HotPlug".

However, DO NOT replace a HotPlug disk drive until a controlled shutdown of the operating system has been performed.

Hardware HotPlug Procedure

To replace a disk drive in the server, grasp the tab at the bottom of the cam latch on the selected disk drive, push the button inside the cam latch, and pull the cam latch out and up. The disk drive will unlock. Pull gently until it slides completely free.

The following graphic shows disk features.



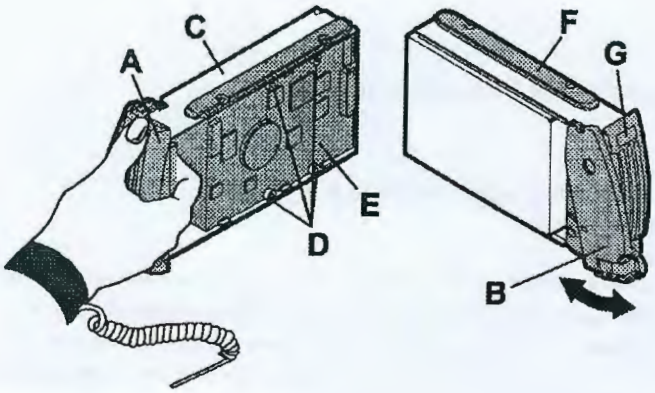
A bezel handle
B cam latch
C carrier frame
D standoffs
E circuit board
F insertion guide
G capacity label

The next graphic depicts disk removal/replacement.

3.018
June

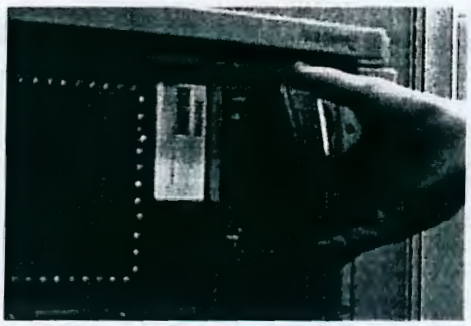
Grasp the tab at the bottom of the cam latch on the selected disk drive, then push the button inside the cam latch and pull the cam latch out and up. The disk drive will unlock. Pull gently until it slides completely free.

The following graphic shows disk features.



A bezel handle
B cam latch
C carrier frame
D standoffs
E circuit board
F insertion guide
G capacity label

The next graphic depicts disk removal/replacement.



ROS Nº 02/2005 - CN
CPMI - CORREIOS
0051
Fls:
3701
Doc:

3.019 June

(for 1 way mirroring)

OR

```
# lvreduce -m 1 -A n -k <LV name> /dev/dsk/cXtXcX <pvkey#>&
```

(for 2way mirroring)

For example, enter:

```
# lvreduce -m 0 -A n -k /dev/vg00/lvol4 /dev/dsk/c2t4d0 1&
```

The following message will appear:

```
Logical volume /dev/vg00/lvol4 has been successfully reduced.
lvlnboot: Logical Volume has no extents.
```

NOTE It is important to include the ampersand (&) at the end of the command line. Otherwise, the *lvreduce* process will hang, and you will need terminal control to negate the command. Once the 'successfully reduced' message has been generated, manually end the process using the *kill -9* command.

Step 1. Use the *ps* command to find the PID for the *lvreduce* process.

```
# ps -ef | grep lvreduce
```

Step 2. Manually end the process with the *Kill -9* command (It may take several minutes for the process to end.).

```
# kill -9 <PID>
```

Step 3. Repeat steps 4 and 5 for all logical volumes.

Step 4. With all logical volumes reduced, now reduce the volume group using the *vgreduce* command. For example:

```
# vgreduce /dev/vg00 /dev/dsk/c2t6d0
```

CAUTION The *vgreduce* procedure may take a long time to complete. Do NOT terminate this process.

Step 5. Update the disk BDRA using the *lvlnboot* command.

lvlnboot -R

Step 6. Proceed to the *HotPlug Hardware Procedure* to remove the bad disk drive from the server.

HotPlug Hardware Procedure

CAUTION Disk Drives can be removed or installed with the server still powered on. This is referred to as a "manual HotPlug".

To remove a disk drive from the server, perform the following step:

3020 June

```
   00003       0             00003 current       1             00003 current
   00004       0             00004 current       1             00004 current
   00005       0             00005 current       1             00005 current
   00006       0             00006 current       1             00006 current
   00007       0             00007 current       1             00007 current
   00008       0             00008 current       1             00008 current

(etc.)


# lvdisplay -v /dev/vg00/lvol1
--- Logical volumes ---
LV Name                     /dev/vg00/lvol1
VG Name                     /dev/vg00
LV Permission               read/write
LV Status                   available/syncd
Mirror copies               1
Consistency Recovery        MWC
Schedule                    parallel
LV Size (Mbytes)            256
Current LE                  64
Allocated PE                128
Stripes                     0
Stripe Size (Kbytes)        0
Bad block                   off
Allocation                  strict/contiguous
IO Timeout (Seconds)        default

   --- Distribution of logical volume ---
   PV Name             LE on PV  PE on PV
   /dev/dsk/c1t6d0     64        64
   /dev/dsk/c2t6d0     64        64

   --- Logical extents ---
   LE    PV1                 PE1   Status 1 PV2                 PE2   Status 2
   00000 /dev/dsk/c1t6d0     00000 current  /dev/dsk/c2t6d0     00000 current
   00001 /dev/dsk/c1t6d0     00001 current  /dev/dsk/c2t6d0     00001 current
   00002 /dev/dsk/c1t6d0     00002 current  /dev/dsk/c2t6d0     00002 current
   00003 /dev/dsk/c1t6d0     00003 current  /dev/dsk/c2t6d0     00003 current
   00004 /dev/dsk/c1t6d0     00004 current  /dev/dsk/c2t6d0     00004 current
   00005 /dev/dsk/c1t6d0     00005 current  /dev/dsk/c2t6d0     00005 current
   00006 /dev/dsk/c1t6d0     00006 current  /dev/dsk/c2t6d0     00006 current
   00007 /dev/dsk/c1t6d0     00007 current  /dev/dsk/c2t6d0     00007 current
   00008 /dev/dsk/c1t6d0     00008 current  /dev/dsk/c2t6d0     00008 current
```

The *pvkey* stuatus (0 or 1 in this example) shown in the first command, maps to the device file names (*/dev/dsk/c1t6d0* or */dev/dsk/c2t6d0*) in the second command under columns *PV1* and *PV2*, respectively.

Step 5. Reduce any logical volumes that have mirror copies on the faulty disk drive so that they no longer mirror onto that disk drive (note the *-A n* option):

```
# lvreduce -m 0 -A n -k <LV name> /dev/dsk/cXtXcX <pvkey#>&
```


ECT Nº 03/2005 - GN
CPMI - CORREIOS
0052
Fls:
Doc: 3701

WARNING:

```
VGDISPLAY: WARNING: COULDN'T QUERY PHYSICAL VOLUME "/DEV/DSK/cXtXdX"
THE SPECIFIED PATH DOES NOT CORRESPOND TO PHYSICAL VOLUME ATTACHED TO THE
VOLUME GROUP.

VGDISPLAY: WARNING: COULDN'T QUERY ALL OF THE PHYSICAL VOLUMES.
```

If you see these messages, the disk was defective at the time the volume group was activated. Remove the bad disk as described in step 9 of this procedure, then follow the instructions in for replacing the disk and perform the *HotSwap Procedure for Unattached Physical Volumes* described there.

Otherwise, the disk drive became defective after *vgchange* was run. Proceed to Step 2.

Step 2. Display the names of all the logical volumes on this volume group with the *vgdisplay* command. For example:

```
#vgdisplay /dev/vg00
```

Step 3. Determine which logical volumes have mirrors with the *lvdisplay* command. For example:

```
#lvdisplay /dev/vg00/lvol# | grep -ie "LV Name" -e "Mirror"
```

Step 4. Determine the *pvkey* command status for the mirrored logical volume, again using the *lvdisplay* command with the *-k* option. Compare the output to the *lvdisplay* command with the *-v* option to determine the device file to *pvkey* mapping. For example,

```
# lvdisplay -v -k /dev/vg00/lvol1
--- Logical volumes ---
LV Name                     /dev/vg00/lvol1
VG Name                     /dev/vg00
LV Permission               read/write
LV Status                   available/syncd
Mirror copies               1
Consistency Recovery        MWC
Schedule                    parallel
LV Size (Mbytes)            256
Current LE                  64
Allocated PE                128
Stripes                     0
Stripe Size (Kbytes)        0
Bad block                   off
Allocation                  strict/contiguous
IO Timeout (Seconds)        default

   --- Distribution of logical volume ---
   PV Name            LE on PV  PE on PV
   /dev/dsk/c1t6d0    64        64
   /dev/dsk/c2t6d0    64        64

   --- Logical extents ---
   LE    PV1                PE1   Status 1 PV2                PE2   Status 2
   00000      0             00000 current       1             00000 current
   00001      0             00001 current       1             00001 current
   00002      0             00002 current       1             00002 current
```

ECT 3.022 June

HotPlug Disk Drive Removal

The internal disk drives (up to four) are located at the front right side of the server (as you are facing it). When proper software and hardware procedures are followed, internal disk drives can be removed and replaced while the server is running.

The procedures in this section are in two parts, a HotSwap Software Procedure and a HotPlug Hardware Procedure, for removing the disk from the server.

Before starting these procedures, you must have an up-to-date configuration backup file. Configuration backup is performed by default each time an LVM command changes the LVM configuration. The default backup files path is:

`/etc/lvmconf/base_vg_name.conf.`

The replacement disk drive must be the same product ID as the disk drive that is being replaced.

NOTE HP often uses different manufacturers for disks that have the same product number. The HotSwap and HotPlug procedures will not update the disk drive's internal information to that of the replaced disk drive.

The replacement disk drive will have the same capacity and blocksize as the defective disk because they have the same product number. The only field that can be incorrect is the string specifying the vendor's name. This will not affect the behavior of the LVM. If you desire to update the manufacturer's name, the disks volume group must be deactivated and reactivated.

HotSwap Software Procedure

Perform these software procedural steps to replace a HotPlug disk drive device:

Step 1. Determine whether LVM found the physical volume to be defective when the volume group was activated.

If the volume was defective when the volume group was activated, *vgchange* will generate the following message to the console:

```
WARNING

VGCHANGE: WARNING: COULDN'T ATTACH TO THE VOLUME GROUP PHYSICAL
VOLUME "/DEV/DSK/cXtXdX"

VGCHANGE: WARNING: COULDN'T ATTACH TO THE VOLUME GROUP PHYSICAL
VOLUME "/DEV/DSK/cXtXdX"

THE PATH OF THE PHYSICAL VOLUME REFERS TO A DEVICE THAT DOES NOT
EXIST, OR IS NOT CONFIGURED INTO THE KERNAL.
```

If you are unsure of the status of *vgchange*, check it with the *vgdisplay* command:

#vgdisplay <VG name>

For example:

vgdisplay /dev/vg00

If the disk was defective when the *vgchange* command was entered, the following message will be printed one or more times:

ROS Nº 03/2005 - CN
6PML CORREIOS
Fls: 0053
Doc: 3701

PCI Card Separator/Extractor Replacement

PCI card separator/extractors are located in the Side Service Bay on the PCI Backplane, between PCI cards. PCI card separator/extractors are plastic cards with two tab handles and two LEDs.

To replace a PCI card separator/extractor, perform the following steps:

1. Insert the PCI card separator/extractor into the available slot and slide it into the PCI backplane connector.
2. Be sure the two hook tabs on the PCI card separator/extractor insert into the connector blocks on either side of the PCI backplane.

Once you have completed replacement of the PCI card separator/extractor into the server, perform the following tasks:

- Replace the PCI card, if necessary.
- Power up the server.

3024
fume

PCI Card Separator/Extractor Removal

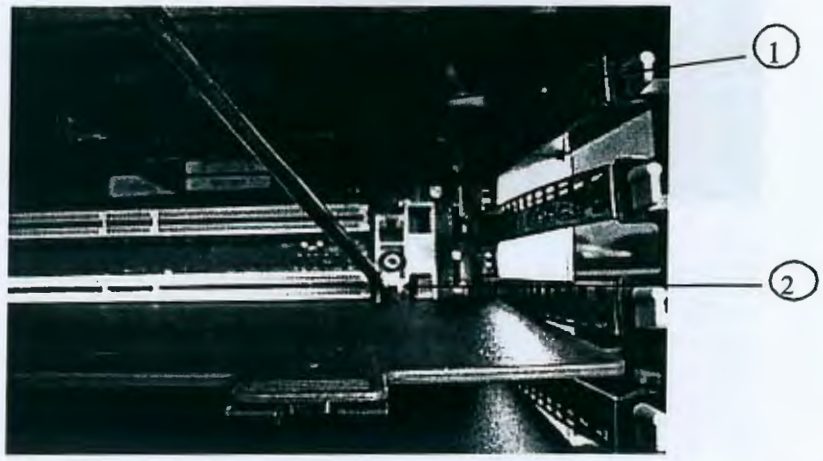
PCI card separator/extractors are located in the Side Service Bay, between the PCI cards. PCI card separator/extractors are plastic cards with two tab handles and two LEDs.

Before removing a PCI card separator/extractor from the server, perform the following tasks:

- Shut down the server.
- Remove the corresponding PCI card.

To remove a PCI card separator/extractor, perform the following steps:

1. Carefully slide a long shaft, medium width, flat blade screw driver (item 1) into the Side Service Bay along the side of the PCI card separator/extractor, and insert it into the slot in the hook tab (item 2).



2. At the point where the PCI card separator/extractor inserts into the PCI backplane connector (item 2), there are two slotted, hook tab connectors on the PCI card separator/extractor, one on either side of the PCI Backplane connector. Press one then the other to disengage the card from the backplane.
3. With the two connection points pressed, slide the PCI card separator/extractor out of the PCI card cage.

NCR 03/2005 - CN
CPMI - CORREIOS
0054
Fls:
Doc:

3025
June

1. Orient the I/O card in its guide and push it into the server until the card connector seats in the I/O Backplane card slot.
2. Connect the I/O cable attached to the I/O card at the rear PCI bulkhead.
3. Connect any ribbon cable connectors attached to the I/O card in the side service bay.

The following graphic shows an I/O card being replaced.

3.026
Juni

Core I/O Replacement

rp54xx Core I/O functions are contained on the GSP and LAN/SCSI cards. Both cards are located on the PCI Backplane in the side service bay. The LAN/SCSI card is in I/O slot 1 and the GSP card is in slot 2.

Before replacing either of the Core I/O cards, perform the following tasks:

- Power down the server.
- Detach all power cords from the server.

NOTE For revision B GSP only, remove *one* of the MAC address labels and place on the rear of the server as shown in the following graphics.

To replace a Core I/O card, perform the following steps:

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0055
Fls:
Doc: 7370

Core I/O Removal

rp54xx Core I/O functions are contained on the GSP revision A/B and LAN/SCSI cards. Both cards are located on the PCI Backplane in the side service bay. The LAN/SCSI card is in I/O slot 1 and the GSP revision A/B card is in I/O slot 2.

Before removing either of the Core I/O cards from the server, perform the following tasks:

- Power down the server.
- Detach all power cords from the server.

To remove a Core I/O card from the server, perform the following steps:

1. Remove all cables attached to the Core I/O card at the rear bulkhead.

NOTE Be sure to label the cables before removing them.

---

2. Disconnect any ribbon cable connectors attached to the Core I/O card in the side service bay.
3. Grasp the edge of the Core I/O card and pull it out of the server.

The following graphic shows both Core I/O cards in the side service bay.

3028
Fls:

Front Bezel Replacement (Two Piece)

The rp54xx server front bezel is divided and hinged on the right (facing the front of the server) side to provide a door for Disk Media Bay access. The server does not have to be turned off to open the access door or to completely remove the bezel.

The Disk Media Bay door encloses the following components:

- HotPlug Disks (A0, A1, and B0, B1).
- Removable Media (CD-ROM drive, etc.).

The left side of the front bezel encloses the following components:

- HotSwap Chassis Fan cover.
- HotSwap Chassis Fan 0.
- HotSwap Power Supplies (up to three).

To attach the bezel, perform the following steps:

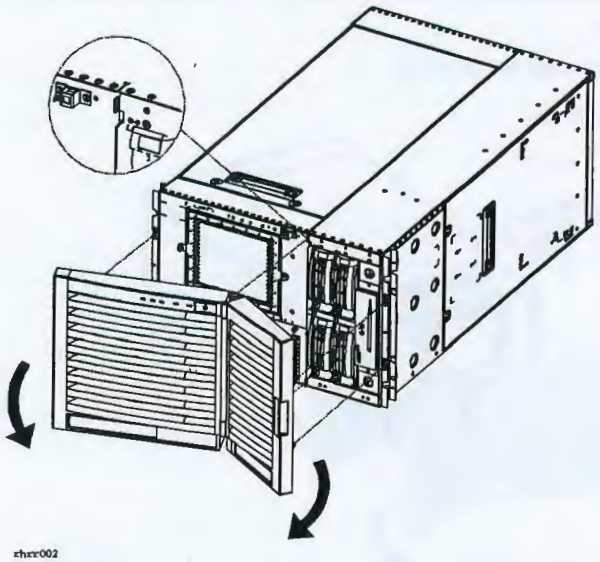
1. Swing the Disk Media access door open so that the plastic pins that go into the metal clips on the Disk Media bay are exposed.

CAUTION The plastic pins holding the bezel on the right side are inserted into metal clips on the Disk Media bay. DO NOT bend the plastic pins or they will break off.

---

2. Holding the bezel with both hands, align the bezel pins with the metal clips on the Disk Media bay and carefully slide the bezel pins into the clips.
3. Attach the left side of the bezel to the server chassis by aligning the bezel pins with the chassis clipsand press the bezel into the chassis until the pins snap into the clips.

   The following graphic shows the front bezel.



zhxr002

4. Swing the Disk Media access door closed and attach it to the right side of the server chassis.

ECT
RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 0056
Doc: 3701

Front Bezel Removal (Two Piece)

The rp54xx server front bezel is divided and hinged on the right (facing the front of the server) side to provide a door for Disk Media Bay access. The server does not have to be turned off to open the access door or to completely remove the bezel.

Opening the door provides access to the following components:

- HotPlug Disks (A0, A1, and B0, B1).
- Removable Media (CD-ROM drive, etc.).

Removing the entire bezel provides access to the components listed above and the following:

- HotSwap Chassis Fan cover.
- HotSwap Chassis Fan 0.
- HotSwap Power Supplies (up to three).

To open the Disk Media access door, grasp the right edge of the door and pull out. The door will swing away from the chassis, exposing the Disk Media Bay.

To remove the entire bezel, perform the following steps:

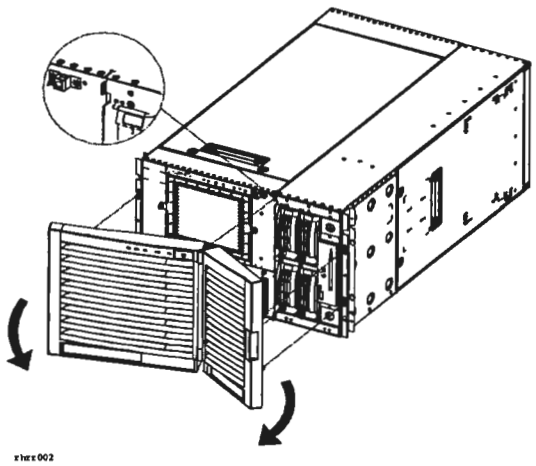
1. Open the Disk Media access door, exposing the plastic bezel pins inserted in the clips at the top and bottom of the Disk Media bay on the left side.
2. Grasp the left side of the bezel and pull it loose.

CAUTION DO NOT try to pull the bezel off of the server at this point. The plastic pins holding the bezel on the right side are inserted in metal clips on the Disk Media bay and if the plastic pins are bent, they will break off.

---

3. Grasp the bezel with both hands and carefully slide the bezel to the left until both plastic pins clear the metal clips on the Disk Media bay.
4. Pull the bezel away from the server and set it aside.

The following graphic shows the front bezel.



3030

Front Bezel Replacement (Single Piece)

The rp54xx server front bezel is hinged on the left (facing the front of the server). The server does not have to be turned off to open or to completely remove the bezel.

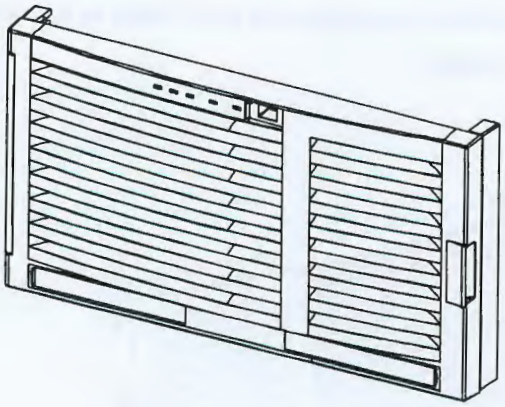
The bezel encloses the following components:

- HotPlug Disks (A0, A1, and B0, B1).
- Removable Media (CD-ROM drive, etc.).
- HotSwap Chassis Fan cover.
- HotSwap Chassis Fan 0.
- HotSwap Power Supplies (up to three).

To attach the bezel, perform the following steps:

1. Screw the bezel hinge to the threaded inserts on the left side of the server.
2. Install the hinge cover by aligning the notch in the top of the cover with the top of the assembly cover and press firmly into place.

The following graphic shows the front bezel.



ROS Nº 03/2005 - CN
CPMI - CORREIOS
0057
Fls:
3701
Doc:

3031 June

Front Bezel Removal (Single Piece)

The rp54xx server front bezel is hinged on the left (facing the front of the server). The server does not have to be turned off to open or to completely remove the bezel.

Opening the door provides access to the following components:

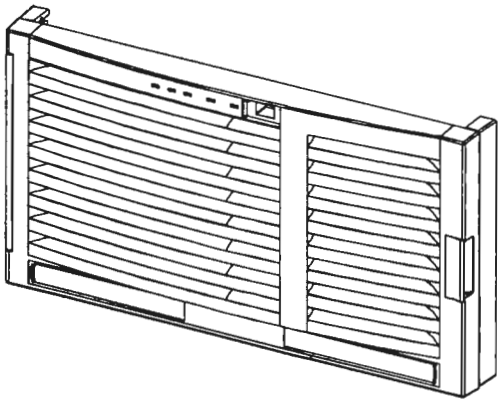
- HotPlug Disks (A0, A1, and B0, B1).
- Removable Media (CD-ROM drive, etc.).
- HotSwap Chassis Fan cover.
- HotSwap Chassis Fan 0.
- HotSwap Power Supplies (up to three).

To open the front bezel, grasp the right edge of the bezel and pull out. The bezel will swing away from the chassis.

To remove the entire bezel, perform the following steps:

1. Open the front bezel and swing it to the left as far as possible.
2. Pry the hinge cover, located on the left side of the server, off the chassis.
3. While supporting the bezel, remove the screws that secure the bezel hinge to the left side of the server.
4. Grasp the left side of the bezel and pull it loose.

The following graphic shows the front bezel.



3.0032
Iure

Side Cover Replacement

The power to the server does not have to be off to replace the side cover. However, operation of the server without the side cover in place can make it susceptible to EMI problems.

Replace the side cover according to the following steps:

1. Grasp the strap handle and insert the tabbed end of the cover into the server chassis slots on the right side of the side service bay.
2. Push the cover into the side service bay opening and fasten the captive T-15 screws that hold the side cover in place.

The following graphic shows the side cover with captive screw locations.

ECT Nº 07/2005 - CN
Chapter
CPMI - CORREIOS
0058
Fls:
3701
Doc:

Side Cover Removal

The Side Cover protects the side service bay. The power to the server does not have to be off to remove the side cover. However, operation of the server without the side cover in place can make it susceptible to EMI problems.

Loosen the captive T-15 screws that hold the side cover in place, then grasp the strap handle and pull the cover away from the server.

The following graphic shows the side cover with captive screw locations.

3.034
fume

Top Cover Replacement

The power to the server does not have to be off to remove or replace the top service bay cover and air baffle. However, operation of the server without the top cover in place can make it susceptible to EMI problems.

Set the air baffle in place over the opening for the top service bay and tighten the captive T-15 screws.

Follow the steps listed below to replace the top cover:

1. Align the tabs on the end of the top cover with the corresponding slots in the chassis and seat the tabs fully into the slots.
2. Seat the top cover in the top of the service bay and tighten the captive T-15 screws that hold the cover in place.

The following graphics show the air baffle and the top service bay cover. The first graphic shows the air baffle.

The second graphic shows the top service bay cover.

ROS Nº 03/2005 - CN
CPMI - CORREIOS
0059
Fls:
3701
Doc:

Top Cover Removal

The power to the server does not have to be off to remove the top cover and air baffle. However, operation of the server without the top cover in place can make it susceptible to EMI problems.

Follow the steps listed below to remove the top cover:

1. Loosen the captive T-15 screws that hold the top cover in place.
2. Grasp the strap handles, raise the cover slightly, and pull the cover toward the front of the server to free the cover tabs from the slots in the chassis. The air baffle will be exposed.

Loosen the captive T-15 screws that hold the air baffle in place then lift the air baffle off of the server.

The following graphics show the top service bay cover and the air baffle. The first graphic shows the top service bay cover.

The second shows the air baffle.

3.036 fls

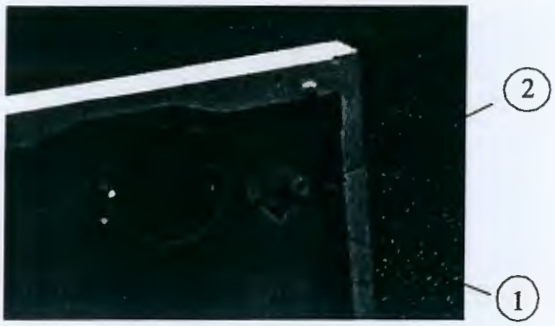
Stand-alone Server Cover Replacement

The rp54xx server can be ordered as a stand-alone unit. In this configuration, the server has a one-piece protective cover over it and sits on a platform with locking wheels attached.

To place the server on its wheeled platform, perform the following procedure:

WARNING **The stand-alone server weights 69 kg (150 lbs). Placing the stand-alone server on its platform requires three people or a suitable lifting device. Failure to heed this precaution can result in serious personal injury or destruction of the server.**

1. Lift the platform and turn both of the spring-loaded, flat-headed pins (item 1) a quarter turn to the right to lock them out of the way before placing the server on the platform.
2. Using a lifting devise or a minimum of three people, lift the server onto the platform. Align the server and platform so that the pins will lock.
3. Reach under the platform, locate the spring-loaded, flat headed pins and turn them one quarter turn to the left to unlock them. Gently slide the server around on the platform until the spring-loaded flat-head pins snap into their holes.
4. Once again, reach under the platform on the right side and fasten both front and back knurl-knobbed, spring-loaded pins (item 2).



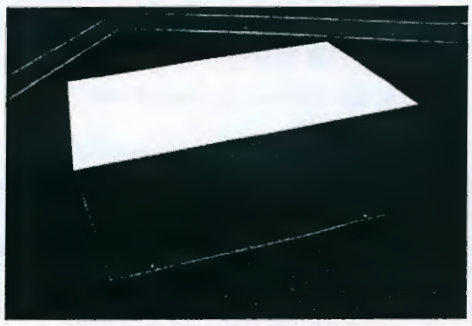
To place the cover on a stand-alone server, perform the following procedures:

1. Set the protective cover on the server and align the holes located near the bottom edge of both sides of the server cover.
2. Fasten the screws (with captive washers) through the cover, into the platform.

The following graphic shows the protective cover.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0060
Fls:
3701
Doc:

The following graphic shows the protective cover.



3.038

Stand-alone Server Cover Removal

The rp54xx server can be ordered as a stand-alone unit. In this configuration, the server has a one-piece protective cover over it and sits on a platform with locking wheels attached.

To remove the cover from a stand-alone server, perform the following procedures:

1. Unfasten and remove the screws (with captive washers) located near the bottom edge of both sides of the server cover.
2. Lift the protective cover off of the server and set it aside.

WARNING **The stand-alone server weights 69 kg (150 lbs). Removing the stand-alone server from its platform requires three people or a suitable lifting device. Failure to heed this precaution can result in serious personal injury or destruction of the server.**

To remove the server from its wheeled platform, perform the following procedure:

1. Facing the front of the server, reach under the platform on the right side and unfasten the knurl-knobbed, spring-loaded pin (item 1). The pin will retract when it is free. Perform the same step at the rear of the server. The rear knurl-knobbed, spring-loaded pin is aligned behind the front pin, but at the rear of the server.

2. From the back of the server, reach under the platform, behind the knurl-knobbed, spring-loaded pin, and locate the flat head of the second spring-loaded pin (item 2). This pin is spring-loaded to stay up and keep the server from sliding on the platform. Pull the pin down and twist one quarter turn to the left to lock the pin down and out of the way. Perform the same step at the front of the server.
3. The server is now free from its wheeled platform and can be removed from it.

WARNING **The stand-alone server weights 69 kg (150 lbs). Removing the stand-alone server from its platform requires three people or a suitable lifting device. Failure to heed this precaution can result in serious personal injury or destruction of the server.**

ROS Nº 03/2005 - CN
CPMI - CORREIOS
0061
Fls:
3701
Doc:

Insert the Server from the Front

rp54xx servers are available in two housings: rack-mounted or stand-alone. Access to servers mounted in an HP-supported rack is covered in this section.

To return the server into the rack, press the rail clips on either side of the server in and push the server into the rack until it stops.

The following graphic shows the server extended and indicates the rail clip location.

3.040
Irene

Individual Component Remove/Replace Instructions

Each component has instructions for removal followed by instructions for replacement.

Extend the Server out the Front

rp54xx servers are available in two housings: rack-mounted or stand-alone. Access to servers mounted in an HP-supported rack is covered in this section.

NOTE Ensure that there is enough area (Approximately 1.5 meters (4.5 ft) to fully extend the server out the front and work on it.

WARNING **Ensure that all anti-tip features (front and rear anti-tip feet installed; adequate ballast properly placed, etc.) are employed prior to extending the server.**

To extend the server, perform the following steps:

1. Remove the four T-25 screws that fasten the server to the rack.
2. Grasp the server chassis and slowly pull forward. The server is fully extended when the rail clips are locked in place. When fully extended, the top and side service bays are fully accessible.

The following graphic shows the server extended and indicates the rail clip location.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0062
Fls:
3701
Doc:

Processor Support Module

Extend the Server out the Front (If Racked)

Stand-alone Server Cover Removal (If Not Racked)

Top Cover Removal

Processor Support Module Removal

Processor Support Module Replacement

Top Cover Replacement

Stand-alone Server Cover Removal (If Not Racked)

Insert the Server from the Front (If Racked)

3.042 frente

PCI I/O Card

Extend the Server out the Front (If Racked)
Stand-alone Server Cover Removal (If Not Racked)
Side Cover Removal
PCI I/O Card Removal
PCI Card Separator/Extractor Removal
PCI Card Separator/Extractor Replacement
PCI I/O Card Replacement
Side Cover Replacement
Stand-alone Server Cover Replacement (If Not Racked)
Insert the Server from the Front (If Racked)

Power Supply

Front Bezel Removal (Single Piece)
Front Bezel Removal (Two Piece)
HotSwap Power Supply Removal
HotSwap Power Supply Replacement
Front Bezel Replacement (Single Piece)
Front Bezel Replacement (Two Piece)

HotSwap Power Converter Fan

HotSwap Power Converter Fan Removal
HotSwap Power Converter Fan Replacement

Platform Monitor

Extend the Server out the Front (If Racked)
Stand-alone Server Cover Removal (If Not Racked)
Top Cover Removal
Platform Monitor Removal
Platform Monitor Replacement
Top Cover Replacement
Stand-alone Server Cover Replacement (If Not Racked)
Insert the Server from the Front (If Racked)

RQS Nº 03/2005 - CN
CORREIOS
0063
Fls:
3701
Doc:

Disk Drive

Front Bezel Removal (Single Piece)

Front Bezel Removal (Two Piece)

HotPlug Disk Drive Removal

HotPlug Disk Drive Replacement

Front Bezel Replacement (Single Piece)

Front Bezel Replacement (Two Piece)

Display Board

Front Bezel Removal (Single Piece)

Front Bezel Removal (Two Piece)

HotSwap Chassis Fan Cover Removal

HotSwap Chassis Fan Removal

Display Board Removal

Display Board Replacement

HotSwap Chassis Fan Replacement

HotSwap Chassis Fan Cover Replacement

Front Bezel Replacement (Single Piece)

Front Bezel Replacement (Two Piece)

Front Bezel

Front Bezel Removal (Single Piece)

Front Bezel Removal (Two Piece)

Front Bezel Replacement (Single Piece)

Front Bezel Replacement (Two Piece)

One Piece Bezel Install

Memory DIMM

Extend the Server out the Front (If Racked)

Stand-alone Server Cover Removal (If Not Racked)

Top Cover Removal

Memory DIMM Removal

Memory DIMM Replacement

Top Cover Replacement

Stand-alone Server Cover Removal (If Not Racked)

Insert the Server from the Front (If Racked)

3.044 June

List of Changeable Parts with Remove and Replace Components

NOTE When viewed in PDF format, component remove/replace instructions may be accessed directly by clicking on the component title listed under each part.

Cardcage Fan

Extend the Server out the Front (If Racked)

Stand-alone Server Cover Removal (If Not Racked)

Side Cover Removal

HotSwap Card Cage Fan Removal

HotSwap Card Cage Fan Replacement

Side Cover Replacement

Stand-alone Server Cover Replacement (If Not Racked)

Insert the Server from the Front (If Racked)

Core I/O

Extend the Server out the Front (If Racked)

Stand-alone Server Cover Removal (If Not Racked)

Side Cover Removal

Core I/O Removal

Core I/O Replacement

Side Cover Replacement

Stand-alone Server Cover Replacement (If Not Racked)

Insert the Server from the Front (If Racked)

HotSwap Chassis Fan

Front Bezel Removal (Single Piece)

Front Bezel Removal (Two Piece)

HotSwap Chassis Fan Cover Removal

HotSwap Chassis Fan Removal

HotSwap Chassis Fan Replacement

HotSwap Chassis Fan Cover Replacement

Front Bezel Replacement (Single Piece)

Front Bezel Replacement (Two Piece)

RQS Nº 03/2005 - CN
CORREIOS
0064
Fls:
3701
Doc:

3.045
June

7 Removing and Replacing Components

The following list of parts can be changed when required to keep the system running properly. The remove/replace components shown under each part indicates the path required for access to each.

3.046
fls.

PROCESSO Nº 03/2005 - CN
CPMI - CORREIOS
0065
Fls:
3701
Doc:

3.047 June

Fan, Power Supply, and Disk LED States

Type	Status	State
Fan	On Amber	State: ▯ Fan Failure
	Off	State: ▯ Normal operation
Power Supply	On Green	State: ▯ Normal operation
	Off	State: ▯ Power Supply Failure
Disk Activity	On Green or Flashing Green	State: ▯ Normal Activity
	Off	State: ▯ No Activity - Normal
Disk Attention	On Amber	State: ▯ Ready for HotPlug
	Off	State: ▯ Normal

3.048

LAN/SCSI LED States

Type	Status	State
LAN Upper	On Green - or - Flashing Green	State: ▯ 100bT Mode
	On Amber - or - Flashing Amber	State: ▯ 10bT Mode
LAN Lower	On Green - or - Flashing Green	State: ▯ LAN Transmit
SCSI Upper	On Green	State: ▯ LVD Mode
	Off	State: ▯ Single Ended Mode
SCSI Lower	On Amber	State: ▯ Termpower Present
	Off	State: ▯ Termpower Absent

ROS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 0066
Doc: 3701

GSP - Revision B

Type	Status	State
GSP Upper	On Green	State: ▯ GSP Power OK
	Flashing Green	State: ▯ GSP LAN receive
	On Red	State: ▯ GSP Failure
GSP Lower	On Amber	State: ▯ 10 Base-T Link OK
	Flashing Amber	State: ▯ 10 Base-T Activity
	On Green	State: ▯ 10 Base-T Link OK
	Flashing Green	State: ▯ 10 Base-T Activity

3.050 fls

GSP LED States

GSP - Revision A

Type	Status	State
GSP Upper	On Green	State: ▯ GSP Power OK
	Flashing Green	State: ▯ GSP LAN receive
	On Red	State: ▯ GSP Failure
GSP Lower	On Green	State: ▯ Link OK
	Flashing Green	State: ▯ GSP LAN transmit
	On Red	State: ▯ GSP Failure

03/2005 - CN
CPMI - CORREIOS
0067
Fls:
3701
Doc:

Power (green)	Attention (amber)	State
Off	Off	State: ▯ Slot available
Power (green)	Attention (amber)	State
Off	Flashing	State: ▯ Fault detected ▯ Power off

3052 June

Expansion I/O LED States

Power (green)	Attention (amber)	State
On	On	State: ▯ Slot selected <or> slot located ▯ Power on Action: ▯ Not ready for OLRAD
Power (green)	Attention (amber)	State
On	Off	State: ▯ Normal operation
Power (green)	Attention (amber)	State
On	Flashing	State: ▯ Fault detected ▯ Power on
Power (green)	Attention (amber)	State
Off	On	State: ▯ Slot selected <or> slot located ▯ Power is off Action: ▯ Ready for OLRAD

ROS Nº 03/2005 - CN
CPMI - CORREIOS
0068
Fls:
3701
Doc:

3.053
Irene

Power (green)	Attention (amber)	State
Off	Flashing	State: ▯ Fault detected ▯ Power off
Off	Off	State: ▯ Slot available

ECT 3.054 June

PCI I/O LED States

Power (green)	Attention (amber)	State
On	Off	State: ▯ Normal operation
On	On	State: ▯ Slot selected <or> slot located ▯ Power on Action: ▯ Not ready for OLRAD
Off	On	State: ▯ Slot selected <or> slot located ▯ Power is off Action: ▯ Ready for OLRAD
On	Flashing	State: ▯ Fault detected ▯ Power on

RQS nº 03/2005 - CN - Chapter 26
CPMI - CORREIOS
0069
Fls:
3701
Doc:

Run (Green)	Attn (Amber)	Fault (Red)	Description
Off	Flashing	On	State: ▯ Boot failed ▯ OS not up and running, PDC has detected a failure that is preventing boot from occurring. ▯ Non-critical error detected (ie. fan failure, power supply failure) Action: ▯ 1. Check chassis logs ▯ 2. Read console messages for indications of problems ie. warnings from PDC
Off	Flashing	Flashing	This is an invalid indication. Check the server's LEDs and try again.
	On		Any combination with amber on is an invalid indication since amber is never on solid.

Run (Green)	Attn (Amber)	Fault (Red)	Description
Off	Off	On	State: ▯ Boot failed ▯ OS not up and running, PDC has detected a failure that is preventing boot from occurring. Action: ▯ 1. Check chassis error logs ▯ 2. Read console messages for indications of problems ie. warnings from PDC
Off	Off	Flashing	This is an invalid indication. Check the server's LEDs and try again.
Off	Flashing	Off	State: ▯ No code is executing (PDC, OS or Diagnostics) ▯ Non-critical error detected (ie. fan failure, power supply failure) (Double fault situation) Action: ▯ Cannot execute PDC. If more than one processor installed, the problem is most likely a failed system board. If only one processor installed, problem could be either the processor or system board. ▯ Check chassis error logs to determine the source of non-critical error.

IKOS Nº: 03/2005 - CN
CPMI - CORREIOS
0070
Fls:
3701
Doc:

Run (Green)	Attn (Amber)	Fault (Red)	Description
Off	Off	Off	State: ▯ A) If Power LED Off ▯ B) If Power LED Flashing ▯ C) If Power LED On Action: ▯ A) Check Power Supply switches and LEDs ▯ Power supply switches should be on and LEDs should be on to indicate presence of AC. If Power Supply LEDs are on and the Front Panel LED is off, replace Power Monitor. ▯ Check AC power at source ▯ B) Turn Front Panel Power Switch on - LED should be on solid ▯ If LED continues to flash, system has been remotely powered off by the service processor or the power monitor has failed. ▯ Execute service processor PC command: type CTRL B, log into the service processor, and type PC at the prompt. ▯ If this doesn't cause the LED to go on solid, problem is most likely with the power monitor. ▯ C) Cannot execute PDC. If more than one processor installed, the problem is most likely a failed system board. If only one processor installed, problem could be either the processor or system board.

3058 fls

Run (Green)	Attn (Amber)	Fault (Red)	Description
Flashing	Flashing	On	State: ▯ Boot failed ▯ Executing non-OS code. ▯ Non-critical error detected (ie. fan failure, power supply failure) Action: ▯ 1. Check chassis error logs ▯ 2. Read console messages for indications of problems ie. warnings from PDC
Flashing	Flashing	Flashing	State: ▯ Unexpected reboot/system recovering. ▯ Executing non-OS code. ▯ Non-critical error detected (ie. fan failure, power supply failure) Action: ▯ 1. Check chassis error logs ▯ 2. Read console messages for indications of problems ie. warnings from PDC

Chapter 6 03/2005 - CN
CPMI - CORREIOS
0071
Fls:
Doc: 3701

Run (Green)	Attn (Amber)	Fault (Red)	Description
Flashing	Off	On	State: ▯ Boot failed ▯ Executing non-OS code. Action: ▯ 1. Check chassis error logs ▯ 2. Read console messages for indications of problems ie. warnings from PDC
Flashing	Off	Flashing	State: ▯ Unexpected reboot occurred ▯ Executing non-OS code. Action: ▯ 1. Check chassis error logs ▯ 2. Read console messages for indications of problems ie. warnings from PDC
Flashing	Flashing	Off	State: ▯ Executing non-OS code. ▯ Non-critical error detected (ie. fan failure, power supply failure) Action: ▯ Read chassis error logs starting at entry 0 to determine cause of flashing amber LED and fix problem.

3.060
frente

Run (Green)	Attn (Amber)	Fault (Red)	Description
Flashing	Off	Off	State: ▯ Executing non-OS code - no problems detected ▯ System may be hung or waiting for BCH response ▯ Potential causes could be PDC never executed (problem with fetching code from PDH), HPMC while PDC was configuring system. Action: ▯ Check console for pending responses ▯ If system appears to be hung, execute TC from GSP prompt and check Last Boot Log for details of previous boot attempt. Pay attention to time stamps to ensure Last Boot Log reflects last boot attempt. ▯ If necessary, bring system down to minimum configuration, processors, memory, I/O, and troubleshoot.

ECT Nº 03/2005 - CN
CPMI - CORREIOS
0072
Fls:
3701
Doc:

3.061 fiere

Run (Green)	Attn (Amber)	Fault (Red)	Description
On	Flashing	On	This is an invalid indication. Check the server's LEDs and try again.
On	Flashing	Flashing	State: ▯ System running, and ▯ A) unexpected reboot occurred, and ▯ B) a non-critical error has been detected Action: ▯ A) Check chassis error logs to determine probable cause of system crash (either HPMC or HP-UX System Panic) ▯ A) Check GSP console logs for potential error messages from the OS (ie. Panic messages) ▯ B) Check chassis error logs to determine probable cause of non-critical error ▯ B) Check Sentinel logs for probable cause of non-critical error

3.062 fls

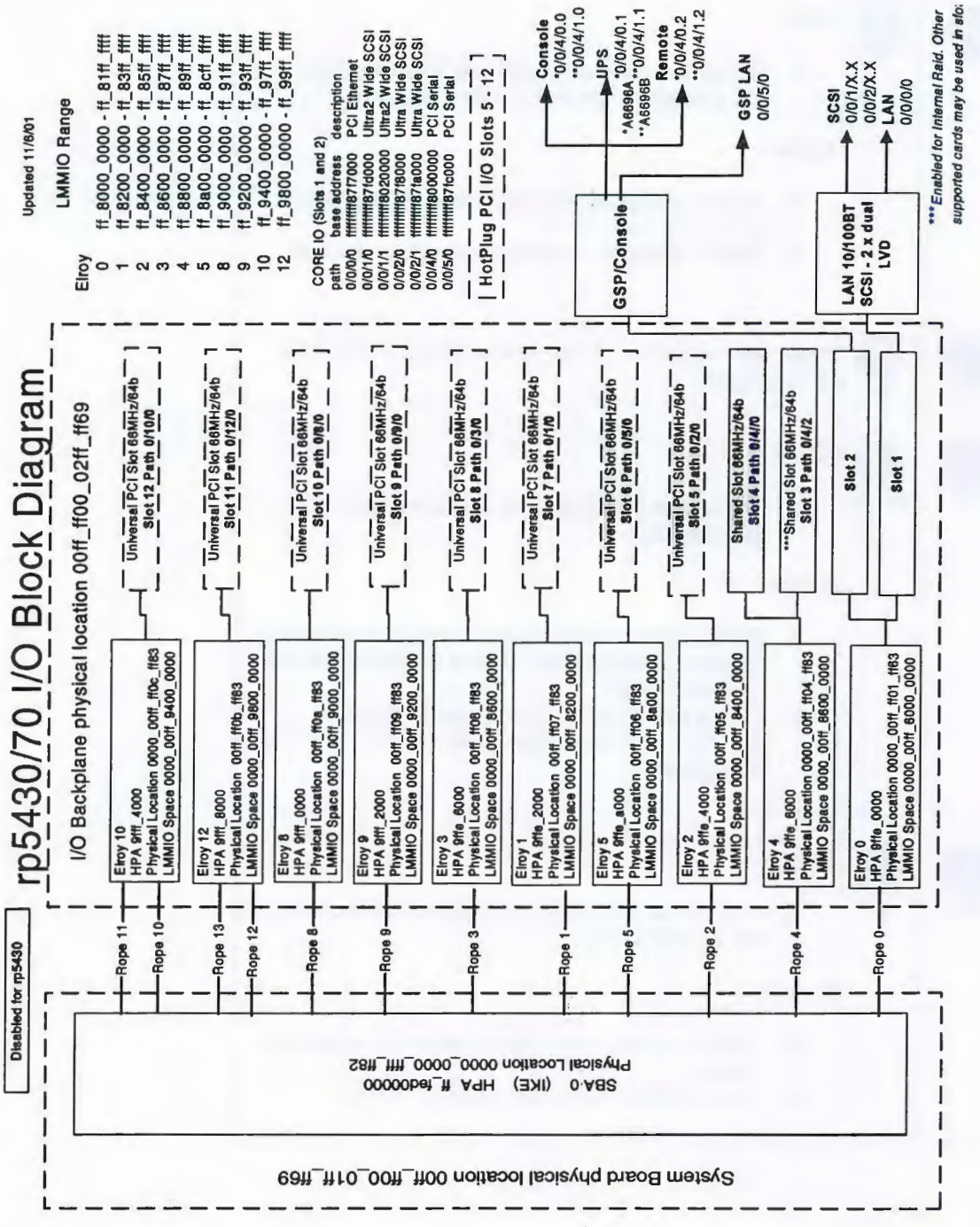
Run/Attention/Fault LED States

Run (Green)	Attn (Amber)	Fault (Red)	Description
On	Off	Off	State: ▯ System running normally. You should expect an OS prompt, if not, system may be hung. Action: ▯ Attempt to get system prompt to determine if system is hung. ▯ Talk to customer to determine reason for call.
On	Off	On	This is an invalid indication. Check the server's LEDs and try again.
On	Off	Flashing	State: ▯ The system crashed and rebooted itself successfully Action: ▯ Check chassis error logs to determine probable cause of system crash (either HPMC or HP-UX System Panic) ▯ Check service processor console logs for potential error messages from the OS (ie. Panic messages)
On	Flashing	Off	State: ▯ There was a system interruption that did not take the system down Action: ▯ Check chassis error logs to determine probable cause ▯ Check Sentinel logs for probable cause

RQS Nº 03/2005 - CN
CORREIOS
0073
Fls:
3701
Doc:

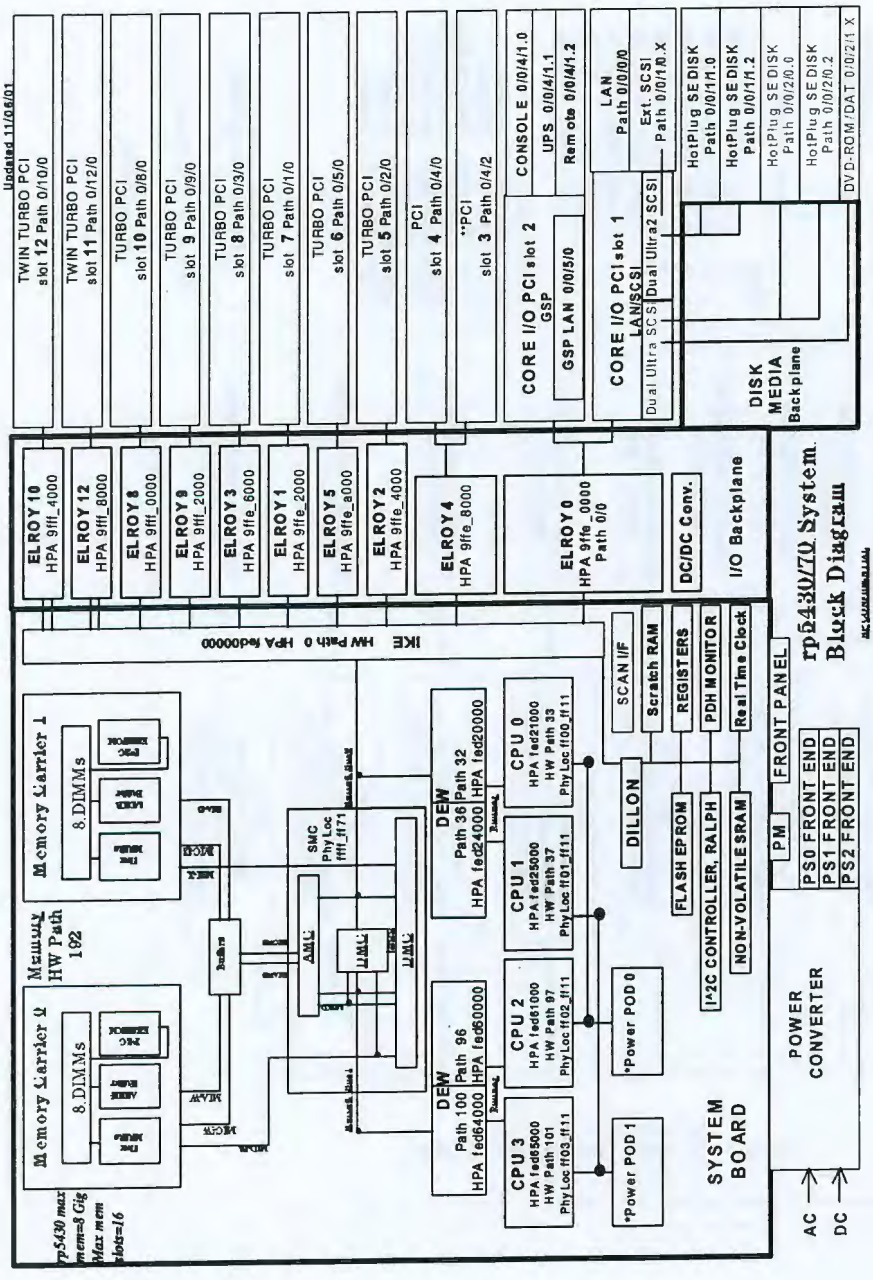
3063
bum

rp5430 and rp5470 I/O Block Diagram



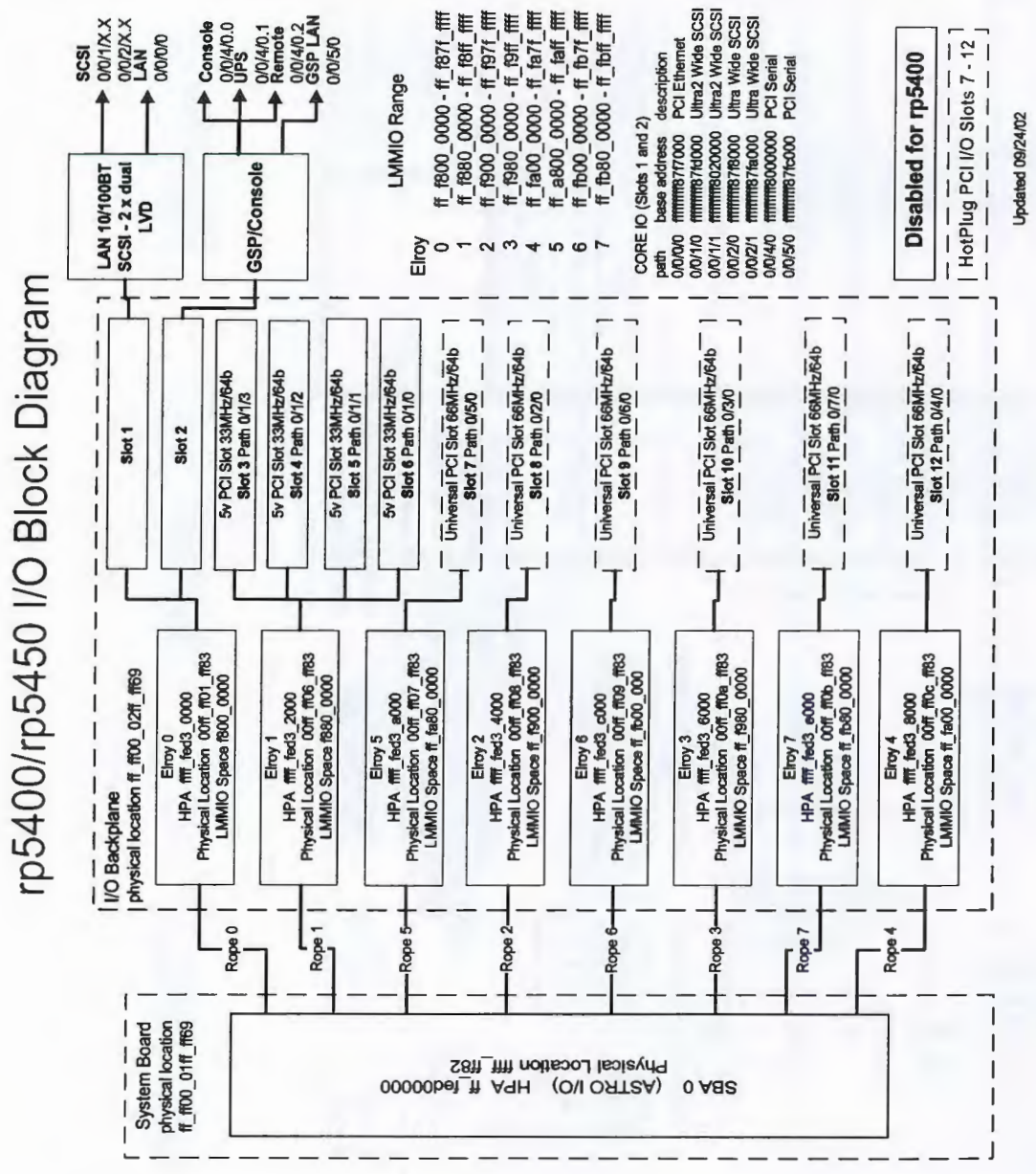
3.064 Irene

rp5430 and rp5470 System Block Diagram



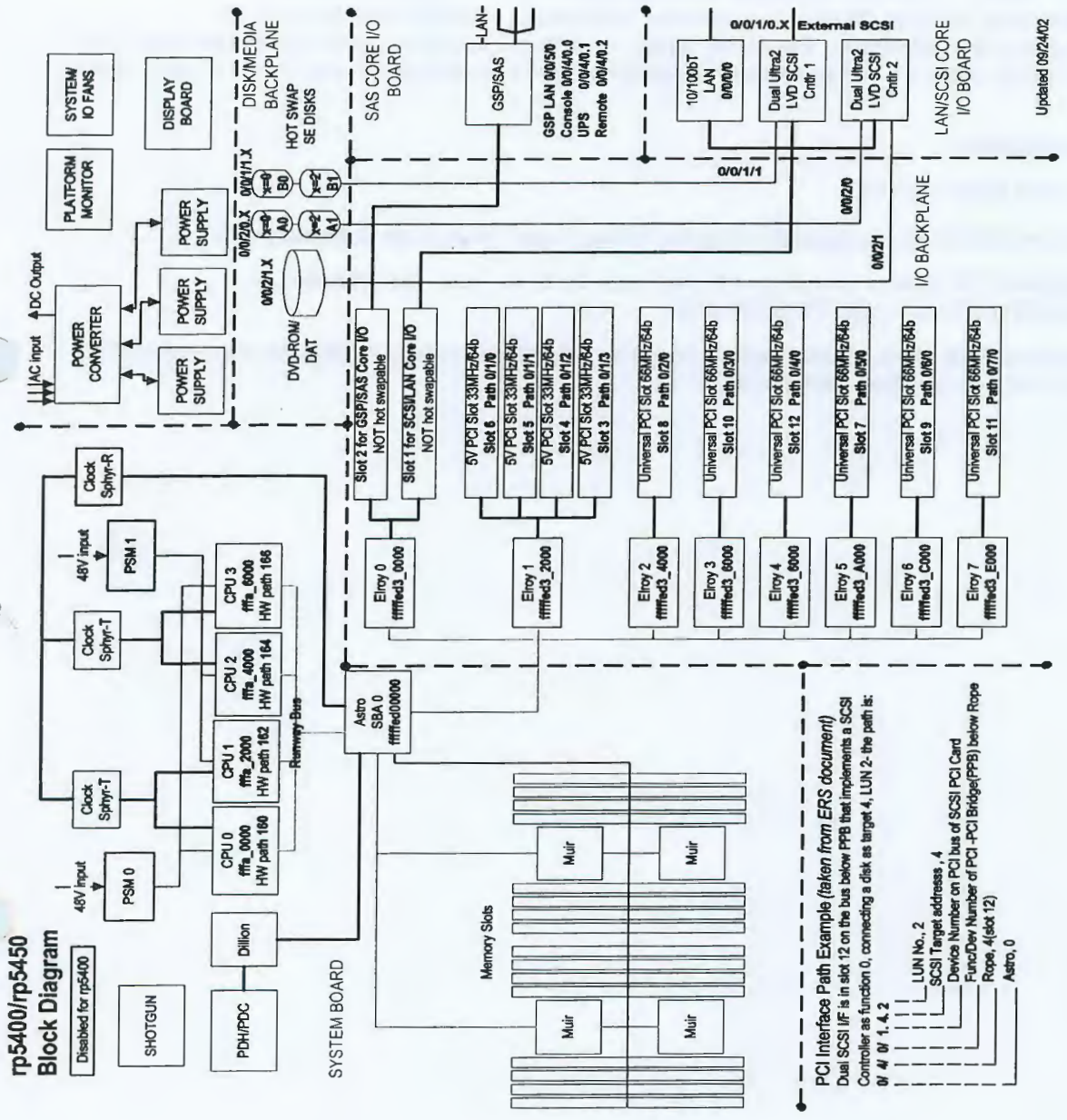
POS Nº 65/2005 - CN
CPMI - CORREIOS
0074
Fls:
Doc: 3701

rp5400 and rp5450 I/O Block Diagram



3.066
June

rp5400 and rp5450 System Block Diagram



IRQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 0075
Doc: 3701

Example 6-1 Chassis Log: Reporting Entity Type = System Firmware

```
Log Entry #   0 :SYSTEM NAME: fesrhapgspDATE: 12/08/2000 TIME: 23:46:22ALERT LEVEL: 6
= Boot possible, pending failure - action requiredSOURCE: 3 = PDHSOURCE DETAIL: 0 =
unknown, no source stated   SOURCE ID: 3PROBLEM DETAIL: 0 = no problem detailCALLER
ACTIVITY: 1 = test   STATUS: 0CALLER SUBACTIVITY: 71 = implementation
dependentREPORTING ENTITY TYPE: 0 = system firmware   REPORTING ENTITY ID:
030x0000306030031710 00000000 000000FE type  0 = Data Field Unused0x5800386030031710
0000640B 08172E16 type 11 = Timestamp 12/08/2000 23:46:22Type CR for next entry, Q CR
to quit.
```

Using the example above:

Step 1. The last 4 digits are 1710.

Step 2. This is an rp5450 so use Appendix B in the *Interpreting Chassis Logs in Detail* guide.

Step 3. Using the FIND feature to look up 1710 in Appendix B, we learn the definition is CC_BOOT_INVALID_SPHYR_SETTINGS.

Step 4. The appropriate action in this example would be to verify the switch settings on the system board are set correctly for the installed CPU's.

3.068
Bruno

2. The problem is with fan #4.
3. The problem is a fan failure.
4. The fan failed on April 15, 1999 at 9:29 PM.

In this example, fan #4 should be replaced to correct the problem.

Interpreting Chassis Logs Using the chassis_code.codes File

For chassis logs generated by system firmware (Reporting Entity Type 0), use the chassis_code.codes file for chassis code definitions. Each revision of system firmware (AKA Processor Dependent Code or PDC) has a unique chassis_code.codes file. This file is not part of either the PF_Cxxxxx or PHSS_xxxxx server firmware patches. The chassis_code.codes files appear in the appendices of the *Interpreting Chassis Logs in Detail* guide.

The definition of a PDC reported chassis code is determined by locating either the last four digits of a chassis log or the last three digits of a selftest chassis code in the appropriate chassis_code.codes file. Refer to the *Interpreting Chassis Logs in Detail* guide for definition and examples of selftest chassis codes.

NOTE Be sure to use the appropriate appendix as the PDC for rp5400/rp5450 is different than PDC for rp5470. Using the wrong appendix may result in a mis-interpretation of the chassis code.

To quickly learn the definition of a PDC reported chassis code, follow these four steps:

Step 1. Determine either the last 4 digits of the hex chassis code or the last 3 digits of the selftest chassis code.

Step 2. Go to the appropriate appendix in the *Interpreting Chassis Logs in Detail* guide.

Step 3. Locate the chassis code that matches the last 3 or 4 digits. If viewing via web browser or Adobe Acrobat, use the FIND feature to locate the chassis code.

Step 4. Take action as appropriate.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 0076
Doc: 3701

3.069 Brunel


```
        HP Guardian Service Processor Command Interface
        Type HE to get the list of available commands

fesrhapgsp:
ALERT LEVEL: 6=Boot possible, pending failure or environmental problem - action required
SOURCE: 6=platform - SOURCE DETAIL: 3=cabinet fan
PROBLEM DETAIL: 4=fan failure
GSP> sl

SL

Which buffer are you interested in :
Incoming, Activity, Error, Current boot or Last boot ? (I/A/E/C/L) e
e

Do you want to set up filter options on this buffer ? (Y/[N]) n
n

Type + CR and CR to go up (back in time),
Type - CR and CR to go down (forward in time),
Type Q CR to escape.

Log Entry #   0 :
ALERT LEVEL: 6=Boot possible, pending failure or environmental problem - action required
REPORTING ENTITY TYPE: 2=power monitor - REPORTING ENTITY ID: 00
CALLER ACTIVITY: 4=monitor - CALLER SUBACTIVITY: 05=fan
SOURCE: 6=platform - SOURCE DETAIL: 3=cabinet fan - SOURCE ID: 04
PROBLEM DETAIL: 4=fan failure - ACTIVITY STATUS: F
Data  0 : Low=00000000 : High=00000000 - type  0 = Data Field Unused
Data  1 : Low=0F151D08 : High=00006303 - type 11 = Timestamp 04/15/1999 21:29:08


q

fesrhapgsp:
ALERT LEVEL: 6=Boot possible, pending failure or environmental problem - action required
SOURCE: 6=platform - SOURCE DETAIL: 3=cabinet fan
PROBLEM DETAIL: 4=fan failure
GSP> co

CO

You are now leaving the Guardian Service Processor Command Interface
and returning to the console mode.  Type Ctrl B to reactivate it.

Main Menu: Enter command or menu >
```

Key FRU Identification Fields for Error Chassis Logs

The following fields are for FRU identification.

Alert Level:	How the problem has affected the system operation.
Source:	What major part of the system the alert is referring to (i.e., platform, memory, processor, etc.).
Source Detail:	What sub-part of the system the alert is referring to (i.e., cabinet fan, DIMM, high voltage DC power, etc.).
Source ID:	Specific FRU referred to in Source and Source Detail (i.e., fan #4).
Problem Detail:	Specific problem information (i.e, power off, functional failure, etc.).
Timestamp:	When the problem occurred.

The above sample system alert message shows the following:

1. The problem does not affect booting of the system.

3.070
Irene

Interpreting Service Processor Error Chassis Logs

Accessing the Service Processor Error Chassis Logs will turn the **ATTENTION** LED, blinking on the front panel, OFF.

Chassis Logs (located in the Service Processor) contain low level logging information related to the following 5 categories:

- Incoming log: Contains all chassis logs coming into the Service Processor.
- Activity log: Contains all chassis logs related to system activity.
- Error log: Contains all error chassis logs.
- Current boot log: Contains all chassis logs associated with the current boot.
- Last boot log: Contains all chassis logs associated with the last boot.

The Error Chassis Logs are the ones you need to look at.

Accessing Error Chassis Logs

Execute the following steps to access the Error Chassis Logs.

1. At the system console prompt, type **CTRL B**
2. Enter the Service Processor Login and Password
3. The screen will display: GSP>

   At the GSP> prompt: type SL and press enter
4. The screen will display:

   `Which buffer are you interested in:`
   `Incoming, Error, Current boot, Last boot? (I/A/E/C/L)`, type **E**, and press enter
5. The screen will display:

   Do you want to set up filter options on this buffer? (Y/[N]), type **N**, and press enter
6. The most recent Error Log Entry (Log Entry #0) will be displayed. A carriage return after this will display the next log entry. Type **Q** to stop displaying the log entries. The screen will display: GSP>
7. At the GSP> prompt: type CO, and press enter to return to the console screen.

Example of Accessing Error Logs

Here is an example of accessing the Error Logs from the Boot Console Handler (BCH) Main Menu prompt. User input is shown in *ITALICS*.

```
Main Menu: Enter command or menu > type CTRL B
Service Processor login: System Operator
Service Processor password: ****** (password hidden)

            Welcome to HP Guardian Service Processor
            System Name: fesrhapgsp


fesrhapgsp:
ALERT LEVEL: 6=Boot possible, pending failure or environmental problem - action required
SOURCE: 6=platform - SOURCE DETAIL: 3=cabinet fan
PROBLEM DETAIL: 4=fan failure
GSP>
```


RQS Nº 03/2005 - CN
CPMI - CORREIOS
0077
Fls:
3701
Doc:

3071
Irene

Interpreting System Alerts

Do one of the following:

1. No response: the alert will time out and the system will continue operating.
2. **A** - Responding with the letter **A** will inform the Service Processor that you have seen the entry. The system will continue to operate.
3. **X** - Responding with the letter **X** will inform the Service Processor to disable all future alert messages. This can be re-enabled with a Service Processor command.

Sample System Alert

```
*************************SYSTEM ALERT*************************************
ALERT LEVEL: 6=Boot possible, pending failure or environmental problem - action required
PROBLEM DETAIL: 4=fan failure - SOURCE ID: 04
SYSTEM NAME: fesrhapgsp

MODEL NAME:   MODEL STRING:   S/N:
SPU POWER: ON
ACTIVITY/COMPLETION LEVEL:  0%
SYSTEM BOOT IS PENDING

LEDs:  RUN       ATTENTION     FAULT     REMOTE
       FLASH     OFF           OFF       ON

CALLER ACTIVITY: 4=monitor - CALLER SUBACTIVITY: 05=fan
REPORTING ENTITY TYPE: 2=power monitor - REPORTING ENTITY ID: 00
SOURCE: 6=platform - SOURCE DETAIL: 3=cabinet fan

0x002008646304405F 00000000 00000000 - type  0 = Data Field Unused

0x582008646304405F 00006303 0F151D08 - type 11 = Timestamp 04/15/1999 21:29:08
A: ack read of this entry - X: Disable all future alert messages
Anything else skip redisplay the log entry
->Choice:a
```

Key FRU Identification Fields for System Alerts

The following fields are used for FRU identification.

Alert Level:	How the problem has affected the system operation.
Source:	What major part of the system the alert is referring to (i.e, platform, memory, processor, etc...).
Source Detail:	What sub-part of the system the alert is referring to (i.e, cabinet fan, DIMM, high voltage DC power, etc...).
Source ID:	Specific FRU referred to in Source and Source Detail (i.e, cabinet fan #4).
Problem Detail:	Specific problem information (i.e, power off, functional failure, etc...).
Timestamp:	When the problem occurred.

The above sample system alert shows the following:

1. The problem does not affect system boot.
2. The problem is with platform cabinet fan #4.
3. The problem is a fan failure. Replace fan #4 to correct the problem.
4. The fan failed on April 15, 1999 at 9:29 PM.

ECT 3.072 fls

Step 2. The Source Detail, the Source ID, and the Problem Detail values are all not applicable for the Processor row of the table.

Step 3. The FRU column of the table identifies the FRU as a failing processor.

Step 4. The Action column of the table instructs us to use the Info Menu and PR command of the BCH Main Menu to identify the failing processor.

Here is the output of Step 4 in our example:

```
Main Menu: Enter command or menu > in

---- Information Menu -------------------------------------------

     Command                    Description
     -------                    -----------
     ALL                        Display all system information
     BootINfo                   Display boot-related information
     CAche                      Display cache information
     ChipRevisions              Display revisions of major VLSI
     COprocessor                Display coprocessor information
     FRU                        Display FRU information
     FwrVersion                 Display firmware version
     IO                         Display I/O interface information
     LanAddress                 Display Core LAN station address
     MEmory                     Display memory information
     PRocessor                  Display processor information
     WArnings                 Display selftest warning messages

----
Information Menu: Enter command > pr

PROCESSOR INFORMATION

                          HVERSION  SVERSION              Processor
  Processor    Speed       Model     Model/Op  CVERSION     State
  ---------  --------    --------  --------  --------  -------------
      1      440  MHz    0x05c4     0x0491     2.  0   Active
      3      440  MHz    0x05c4     0x0491     2.  0   Stopped:Nonresponding

  Central Bus Speed (in MHz)    :          82
  Software ID (dec)             : 1635329341
  Software ID (hex)             : 0x6179253d
  Software Capability           : 0x01100000f0

Information Menu: Enter command >
```

Processor #3 is `Stopped:Nonresponding`. Replace Processor #3.

Interpreting System Alerts

System Alerts are reported to the system console when a problem is detected by the Service Processor. These alerts are stored in the Service Processor Error Logs. When this new alert is added to the log file, it will cause the front panel ATTENTION LED to blink.

ROS Nº 03/2005 - CN
CPMI - CORREIOS
0078
Fls:
Doc: 3701

Power Supply Failure Example

```
GSP> sl

SL

Which buffer are you interested in :
Incoming, Activity, Error, Current boot or Last boot ? (I/A/E/C/L) e
e

Do you want to set up filter options on this buffer ? (Y/[N]) n
n

Type + CR and CR to go up (back in time),
Type - CR and CR to go down (forward in time),
Type Q to escape.

Log Entry #   0 :
ALERT LEVEL: 6=Boot possible, pending failure or environmental problem - action required
REPORTING ENTITY TYPE: 2=power monitor - REPORTING ENTITY ID: 00
CALLER ACTIVITY: 4=monitor - CALLER SUBACTIVITY: 04=low voltage power supply
SOURCE: 4=power - SOURCE DETAIL: 4=high voltage DC power - SOURCE ID: 02
PROBLEM DETAIL: A=unexpected - ACTIVITY STATUS: F
Data  0 : Low=00000000 : High=00000000 - type  0 = Data Field Unused
Data  1 : Low=0F152A28 : High=00006303 - type 11 - Timestamp 04/15/1999 21:42:40
```

Problem Analysis

Step 1. Find the Source value. In this example, it is *SOURCE: 4=power*.

Use the **Power** row of the Error Chassis Log-to-FRU Decoder table.

Step 2. Find the Source Detail value. In this example, it is *SOURCE DETAIL: 4=high voltage DC power*.

Use the **High Voltage DC Power** row of the table.

Step 3. Find the Source ID value. In this example, it is *SOURCE ID: 02*.

The failing power supply is Power Supply #2.

Step 4. The Problem Detail for this row is not applicable.

Step 5. The FRU column of the table identifies the FRU as the Power Supply.

The correct action would be to replace Power Supply #2, located in the front of the system.

Processor Failure Example

```
Log Entry #   1 :
ALERT LEVEL: 6=Boot possible, pending failure or environmental problem - action required
REPORTING ENTITY TYPE: 0=system firmware - REPORTING ENTITY ID: 01
CALLER ACTIVITY: 1=test - CALLER SUBACTIVITY: 62=implementation dependent
SOURCE: 1=processor - SOURCE DETAIL: 1=processor general - SOURCE ID: 00
PROBLEM DETAIL: 3=functional failure - ACTIVITY STATUS: 0
Data  0 : Low=00000003 : High=F7000000 - type  0 = Data Field Unused
Data  1 : Low=0F160920 : High=00006303 - type 11 - Timestamp 04/15/1999 22:09:32
```

Problem Analysis

Step 1. Find the Source value. In this example, it is *SOURCE: 1=processor*.

Use the **Processor** row of the Error Chassis Log-to-FRU Decoder table.

3074 fls

Table 6-2 Chassis Log Error to FRU Decoder (Continued)

Chassis Log Field Values and Descriptions from Log Entry					
Source	**Source Detail**	**Source ID**	**Problem Detail**	**FRU**	**Action to Take**
3 - PDH	Not Applicable (N/A)	N/A	N/A	System Board	Replace the System Board.
4 - Power	1 - AC Mains	N/A	9 - Power Off	AC Power	Check that AC is being supplied to all power supplies.
4 - Power	3 - Low Voltage DC Power	CPU Support Module #	N/A	CPU Support Module	Replace the Processor Support Module (on the System Board) referenced in the Source ID.
4 - Power	4 - High Voltage DC Power	Power Supply #	N/A	Power Supply	Replace the Power Supply (in the front of the system behind the bezel) referenced in the Source ID.
6 - Platform	3 - Cabinet Fan	Fan #	N/A	Fan	Replace the Fan referenced in the Source ID.
6 - Platform	6 - Service Processor	N/A	N/A	Core I/O	The Service Processor is on the GSP I/O board. Replace the GSP
6 - Platform	7 - Power Monitor	N/A	N/A	Power Monitor	Replace Platform Monitor card.
7 - Memory	1 - Controller	N/A	N/A	System Board	Replace the System Board.
Memory	4 - SIMM or DIMM	N/A	N/A	Memory DIMM	Isolate to failing DIMM using BCH (IN, ME) and ODE memory diagnostic.
8 - I/O	6 - Disk	N/A	Various Values	Disk Subsyste m	Use BCH commands and ODE diagnostics to check disk subsystem.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0079
Fls: 3701
Doc:

Chassis Code to FRU Decode

This is a guide to identify failing FRUs from System Alerts and Error Chassis Logs. The guide includes the following information:

- Cross-Referencing Chassis Log Errors to rp54xx FRUs
- Interpreting System Alerts
- Interpreting Service Processor Error Chassis Logs

There is a detailed interpretation of Chassis Logs and System Alerts in the *Interpreting Chassis Logs in Detail* guide.

Cross-Referencing Chassis Log Errors to rp54xx FRUs

Use the following table to identify the failing FRU from the Chassis Log information. You can also use the online Error Chassis Log-to-FRU Decoder utility.

1. Read the Chassis Log entry.
2. Match the **SOURCE, SOURCE DETAIL, SOURCE ID,** and **PROBLEM DETAIL** values (see table below) in the Chassis Log entry with the appropriate values in the table.
3. Read the table from left to right.

Use these examples to understand how to identify failing FRUs with the table:

- Power Supply Failure Example
- Processor Failure Example

Table 6-2 Chassis Log Error to FRU Decoder

Chassis Log Field Values and Descriptions from Log Entry					
Source	**Source Detail**	**Source ID**	**Problem Detail**	**FRU**	**Action to Take**
1 - Processor	Not Applicable (N/A)	N/A	N/A	Processor	From BCH Main Menu go to the Info Menu and execute the PR command to determine which processor is not functioning.
2 - Processor Cache	Not Applicable (N/A)	N/A	N/A	Processor	From BCH Main Menu go to the Info Menu and execute the PR command to determine which processor is not functioning.

ECT 3.076 Bruno

Table 6-1 Problem Symptoms and Repair Actions (Continued)

Problem or Symptom	Problem Indicators	Normal Functioning Indicators	Troubleshooting Steps	Potential FRUs
Can't boot to ISL.	Console messages indicating problems booting from the primary or alternate boot path.	• Console messages and prompt indicating you are at ISL.	1. Use BCH commands to verify I/O and presence of valid LIF devices. 2. Use BCH "Warn"command to determine if Boot is disabled. 3. Check for IODC tombstones. 4. Check SP chassis error logs.	• Disk Drive • Disk Media Backplane • LAN/SCSI Board • I/O Backplane
...'t boot HP-UX.	HP-UX boot error messages. RUN LED BLINKING.	• HP-UX boot messages. • HP-UX prompt. • RUN LED on SOLID.	1. Check SP chassis error logs. 2. Run ODE diagnostics.	• Processor • Disk Drive • Disk Media backplane • LAN/SCSI • Corrupt HP-UX

ECT 3.076 Bruno
BOS Nº 03/2005 - CN
CPMI - CORREIOS
0080
Fls:
3701
Doc:

3.077

Table 6-1 Problem Symptoms and Repair Actions (Continued)

Problem or Symptom	Problem Indicators	Normal Functioning Indicators	Troubleshooting Steps	Potential FRUs
No BCH Main Menu prompt.	Front Panel RUN LED is not FLASHING. There is no forward progress chassis codes at the console. There is no BCH Main Menu prompt at the console.	• Flashing RUN LED. • Forward progress chassis codes. • BCH Main Menu prompt.	1. Check for red LED on GSP. If lit red, the problem is with the GSP. 2. Check that the console is properly connected and can communicate with the Service Processor (CTRL B should get you the SP login prompt). 3. Check Service Processor Error logs. Look for entries related to: • Processors • Processor Support Modules (known as low voltage DC supplies in chassis codes. Also known as power pods). • Memory 4. Reduce to minimum configuration and troubleshoot from there.	• Core I/O • Processors • Processor Support Modules • Memory • System Board • Console

3.078 Irene

Table 6-1 Problem Symptoms and Repair Actions (Continued)

Problem or Symptom	Problem Indicators	Normal Functioning Indicators	Troubleshooting Steps	Potential FRUs
System won't power on when Front Panel Power switch is turned on.	Front Panel Power LED stays BLINKING when Power Switch is turned on. ATTENTION LED may be FLASHING.	• Power switch On. • Power LED on SOLID.	1. Check for remote power shutdown via GSP>PC command. 2. *Check Error Chassis Logs*. Look for Error Chassis Log with a Source Detail = Low Voltage DC Power. This indicates a failure of one of the CPU Support Modules. The failing CPU support module is indicated in the Source ID field. 3. Ensure there are 2 working power supplies (1 supply for rp5400). The LED on each supply should be lit. 4. Check to see if GSP can communicate with platform monitor. Execute the following GSP command: GSP>PC You should get power monitor status information. 5. Housekeeping 1 voltage present indication. Check that platform monitor power LED is lit. 6. Platform Monitor functioning. Check platform monitor heartbeat LED is lit.	• Power Supplies • CPU Support Module • Platform Monitor • System Board

Chapter 6 03/2005 - CN
CPMI - CORREIOS
0081
Fls:
3701
Doc:

3.079 June

Troubleshooting and FRU identification

Once you have determined the current system state, you must troubleshoot the system to determine what the problem symptoms are and what repair actions to take.

Problem Symptoms and Repair Actions

Use this guide to assist you in repairing the system by matching the problem symptom with the appropriate troubleshooting step.

Table 6-1 Problem Symptoms and Repair Actions

Problem or Symptom	Problem Indicators	Normal Functioning Indicators	Troubleshooting Steps	Potential FRUs
No indication of Housekeeping voltage present when AC connected and power switch in Standby position.	Front Panel Power LED OFF when AC is plugged into system.	• Power switch Off. • Front Panel POWER LED should be FLASHING to indicate presence of Housekeeping voltage. • Power LED on GSP board should be lit solid green.	1. AC must be present. Check that PDU is plugged in. 2. Ensure there are 2 working power supplies (1 supply for rp5400). The LED on each supply should be lit. 3. Check for Service processor prompt (CTRL B at console).	• No AC present • Power Supplies • Power Converter • System Board • Display Board

3.080
June

Determine Current System State

To determine the current system state of an rp54xx server, first note the state of all LED indicators on the front panel. Processing this information using the decoders provided can greatly reduce the amount of time required to repair a suspected system fault.

The following procedure lists the tools available to aid you in determining the current system state.

Step 1. Determine if you can get a system prompt and if so, what kind of prompt.

Software System	Screen Prompt
Boot Console Handler (BCH)	`Main Menu: Enter command or menu>`
Guardian Service Processor (GSP)	`GSP>`
Initial System Loader (ISL)	`ISL>`
HP UNIX (HP-UX)	*Prompt varies depending on UNIX state*

Step 2. Decode the Run/Attention/Fault LED States.

Step 3. Decode the PCI I/O LED States.

Step 4. Decode the Fan, Power Supply, and Disk LED States.

Step 5. Decode the GSP LED States.

Step 6. Decode the LAN/SCSI LED States.

RQS N° 03/2005 - CN
CPMI - CORREIOS
0082
Fls:
Doc: 3701

6 Troubleshooting

3.082
Fls:

CPMI - CORREIOS
0083
Fls:
3701
Doc:

Removing Users

You can removedisable) a GSP user with the same Security options and access control (SO) command used to add a user.

To remove a user, perform the following steps:

1. Go into the GSP with the ctrl+b entry.
2. At the GSP prompt, enter the Security options and access control (SO) command:

   ```
   GSP> so
   ```

3. The first prompt you will see with the so command is for GSP wide parameters:

   ```
   GSP wide parameters are:
   . Login Timeout: 1 minutes.
   . Number of password Faults allowed: 3
   . Flow Control Timeout: 5 minutes.

   Do you want to modify the GSP wide parameters? (Y / [N]) __
   ```

   At this point you can modify the GSP wide parameters, or continue with removing a user. To remove users, respond N for no.

NOTE You will have to step through each user number until you reach the user to be removed.

4. When you access the number of the user to be removed, you must change the data in the prompts for that number.

   It is important that, at a minimum, you need to modify the User's state to Disabled.

Changing the Default GSP Configuration

This section describes the process of changing GSP default configurations. To change the GSP default configuration, perform the following steps:

1. Go into the GSP with the ctrl+b entry.
2. At the GSP prompt, enter the Default Configuration (dc) command:

   ```
   GSP> dc
   ```

3. Follow the prompts for the dc command, and be sure to have the change information available.

CAUTION When the Security configuration is reset, all users are removed, including the GSP administrator. It also disables the remote. Remote must be re-enabled through the main console using the Enable Remote (er) command.

3.084
fls

To add a user, perform the following steps:

1. Go into the GSP with the ctrl+b entry.
2. At the GSP prompt, enter the Security options and access control (SO) command:

   GSP> so

3. The first prompt you will see with the so command is for GSP wide parameters:

```
GSP wide parameters are:
Login Timeout: 1 minutes.
. Number of password Faults allowed: 3
. Flow Control Timeout: 5 minutes.
Do you want to modify the GSP wide parameters? (Y / [N]) __
```

   At this point you can modify the GSP wide parameters, or continue with adding users. To add users, respond N for no.

NOTE If this is the first time users are being added, the first user added will be the GSP administrator.

If this is not the first time you are adding users (you are adding additional users), you will need to step through all current users to reach the next available user prompt.

---

4. The next prompt that appears will ask the following question:

   Do you want to modify the user number 1 parameters? (Y/[N]/Q to quit) __

   Follow the series of prompts to enter all the required fields for adding a user.

CAUTION Be sure to read each prompt carefully and enter the correct response. A missed or incorrect entry could deny entry to that user.

An example of an added users information would be:

```
. User's Name: Joe Smith
. Organization's Name: IT Support
. Dial-back configuration: Disabled
. Access Level: Operator
. Mode: multiple
. User's state: enabled
```

For the number 1 user, the Access level is administrator. The Mode entry of single only allows entry for that user one time, then access will be denied. A Mode entry of multiple allows unlimited entries into the GSP.

RQS N 03/2005 - CN
CPMI - CORREIOS
0084
Fls:
Doc: 3701

Configuring the Rev B Guardian Service Processor (GSP)

The Rev B Guardian Service Processor (GSP) is a resident processor within the system that allows the local or remote system administrator to monitor and perform administrator functions. This section provides configuration procedures that will instruct you to:

- Configure the LAN port
- Add or delete users (maximum of 20)
- Change the default GSP configuration

Go to the appropriate section for the task that you wish to accomplish.

Configuring the GSP LAN Port

Perform the LAN configuration from the systems local port (either console or the HP secure web console).

NOTE The GSP has a separate LAN port from the system LAN port. It will need a separate LAN drop, IP address, and networking information from the port used by HP-UX.
Before starting this procedure, you will need to know the following information:

- I.P. address (for GSP)
- Subnet mask
- Gateway address
- Hostname (this is used when messages are logged or printed)

To configure the GSP LAN port, perform the following steps:

1. Go into the GSP with the ctrl+b entry.
2. At the GSP prompt, enter the LAN Configuration (lc) command:

```
GSP> lc
```

The lc command will start a series of prompts. Respond to each prompt with the appropriate information.

Adding Users

The GSP can only have a maximum of 20 users (one administrator and 19 operators). By design, the first user added to the GSP becomes the GSP administrator. Only the GSP administrator can add or remove users or change the GSP configuration.

NOTE Before starting this procedure, you will need to know the following information:

- User's name
- Organization's name
- Login name
- User's password

3.086
June

Removing Users

You can remove (disable) a GSP user with the same Security options and access control (SO) command used to add a user.

To remove a user, perform the following steps:

1. Enter the GSP with the ctrl+b entry.
2. At the GSP prompt, enter the Security options and access control (SO) command:

   ```
   GSP> so
   ```

3. The first prompt you see with the so command is for GSP-wide parameters:

   ```
   GSP wide parameters are:
   . Login Timeout: 1 minutes.
   . Number of password Faults allowed: 3
   . Flow Control Timeout: 5 minutes.

   Do you want to modify the GSP wide parameters? (Y / [N]) __
   ```

   At this point you can modify the GSP-wide parameters, or continue with removing a user. To remove users, enter N for no.

NOTE You must step through each user number until you reach the user to be removed.

4. When you access the number of the user to be removed, you must change the data in the prompts for that number.

   It is necessary that, at a minimum, you modify the User's state to Disabled.

Changing the Default GSP Configuration

This section describes the process of changing GSP default configurations. To change the GSP default configuration, perform the following steps:

1. Enter the GSP with the ctrl+b entry.
2. At the GSP prompt, enter the Default Configuration (dc) command:

   ```
   GSP> dc
   ```

3. Follow the prompts for the dc command, and have the change information available.

CAUTION When the Security configuration is reset, all users are removed, including the GSP administrator. The remote is disabled. The remote must be re-enabled through the main console using the Enable Remote (er) command.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0085
Fls: 3701
Doc:

3.087 June

To add a user, perform the following steps:

1. Enter the GSP with the ctrl+b entry.
2. At the GSP prompt, enter the Security options and access control (SO) command:

   GSP> so

3. The first prompt you see with the so command is for GSP-wide parameters:

```
GSP wide parameters are:
Login Timeout: 1 minutes.
. Number of password Faults allowed: 3
. Flow Control Timeout: 5 minutes.
Do you want to modify the GSP wide parameters? (Y / [N]) __
```

   At this point you can modify the GSP-wide parameters or continue adding users. To add users, enter N for no.

NOTE If this is the first time users are being added, the first user added will be the GSP administrator.

If this is not the first time you are adding users (you are adding additional users), you will need to step through all current users to reach the next available user prompt.

---

4. The next prompt that appears will ask the following question:

   Do you want to modify the user number 1 parameters? (Y/[N]/Q to quit) __

   Follow the series of prompts to enter all the required fields for adding a user.

CAUTION Be sure to read each prompt carefully and enter the correct response. A missed or incorrect entry will deny entry to that user.

The following is an example of an added users information:

```
. User's Name: Joe Smith
. Organization's Name: IT Support
. Dial-back configuration: Disabled
. Access Level: Operator
. Mode: multiple
. User's state: enabled
```

For the number 1 user, the Access level is administrator. The Mode entry of single only allows entry for that user one time, then access will be denied. A Mode entry of multiple allows unlimited entries into the GSP.

3.058
fls

Configuring the Rev A Guardian Service Processor (GSP)

The Rev A Guardian Service Processor (GSP) is a resident processor within the system that allows the local or remote system administrator to monitor and perform administrator functions. This section provides configuration procedures that will instruct you to:

- Configure the LAN port
- Add or delete users (maximum of 20)
- Change the default GSP configuration

Go to the appropriate section for the task that you wish to accomplish.

Configuring the GSP LAN Port

Perform the LAN configuration from the systems local port (either console or the HP secure web console).

NOTE The GSP has a separate LAN port from the system LAN port. It will need a separate LAN drop, IP address, and networking information from the port used by HP-UX.
Before starting this procedure, you will need to know the following information:

- I.P. address (for GSP)
- Subnet mask
- Gateway address
- Hostname (this is used when messages are logged or printed).

To configure the GSP LAN port, perform the following steps:

1. Go into the GSP with the ctrl+b entry.
2. At the GSP prompt, enter the LAN Configuration (lc) command:

```
GSP> lc
```

The lc command will start a series of prompts. Respond to each prompt with the appropriate information.

Adding Users

The GSP can only have a maximum of 20 users (one administrator and 19 operators). By design, the first user added to the GSP becomes the GSP administrator. Only the GSP administrator can add or remove users or change the GSP configuration.

NOTE Before starting this procedure, you will need to know the following information:

- User's name
- Organization's name
- Login name
- User's password

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 0086
Doc: 3701

ECT 3.090 Brent

Step 4. When the initial power-up boot process completes in approximately one to five minutes, the BCH main menu will be displayed:

```
---- Main Menu ---------------------------------------------------------------

     Command                              Description
     -------                              -----------
     BOot [PRI|ALT|<path>]                Boot from specified path
     PAth [PRI|ALT|CON|KEY] [<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
     DeBug menu                           Displays debug 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 5. To start the boot process using the primary boot path, enter *BO PRI*, at Boot Console Handler BCH main menu prompt and press **<ENTER>**.

NOTE Booting a system to a UNIX login prompt from BCH main menu can take 20 minutes or longer depending on your software and hardware configuration.

Step 6. Once the system reaches the UNIX login prompt the following will be displayed on the console screen:.

```
HP-UX hprfes A.09.04 U 9000/897 (ttyp2)

login:
```


RQS Nº 03/2005 - CN
CORREIOS
Fls: 0087
Doc: 3701

3.091 June

Step 3. Several self-test boot progress screens will be displayed and will scroll rapidly up the screen. Some tests may pause for up to one minute while the test completes.
The following examples of the forward progress screens are typical of the screens displayed.

Brief

```
********************************* EARLY BOOT VFP ********************************

0x0000180089002300 00000000 00000000

Q/q: quit Virtual Front Panel Display
->Choice:
*********************************************************************************
```

Verbose

```
********************************* EARLY BOOT VFP ********************************
ALERT LEVEL: 0=No failure detected, forward progress
PROBLEM DETAIL: 0=no problem detail - SOURCE ID: 00
SYSTEM NAME: fespre2sas
MODEL NAME:   MODEL STRING:   S/N:
SPU POWER: ON
ACTIVITY/COMPLETION LEVEL:  0%
SYSTEM BOOT IS PENDING

LEDs:  RUN      ATTENTION     FAULT     REMOTE
       FLASH    FLASH         OFF       ON

CALLER ACTIVITY: 1=test - CALLER SUBACTIVITY: A4=implementation dependent
REPORTING ENTITY TYPE: 0=system firmware - REPORTING ENTITY ID: 01
SOURCE: 7=memory - SOURCE DETAIL: 0=unknown, no source stated

0x7000100070001A42 00000000 00000001 - type 15 = Activity Level/Timeout

Q/q: quit Virtual Front Panel Display
->Choice:
```

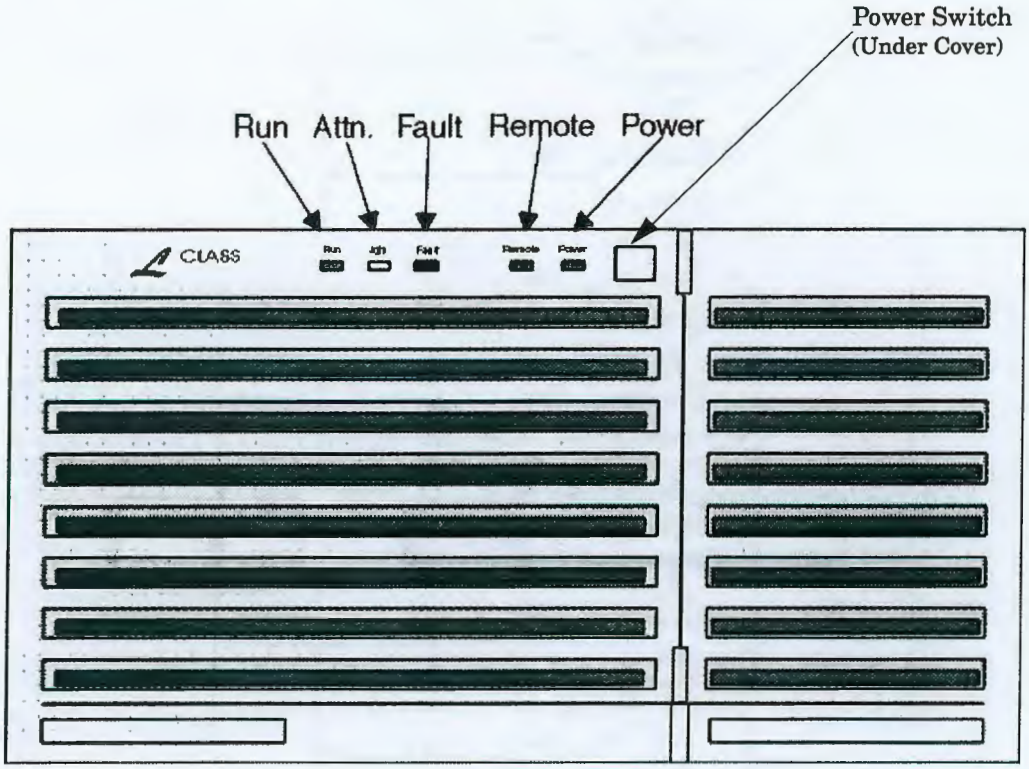
E.C.T. 3.092 Fls: Doc:

Initial Power-up

The following section describes the process of applying power to the rp54xx server and booting the system to the UNIX Login prompt. The amount of time it takes to go through self-test then boot the system will vary widely depending on hardware configuration. The following provides a "typical" procedure. Yours may vary depending on software and hardware installed:

Step 1. Apply AC Power to the system console.

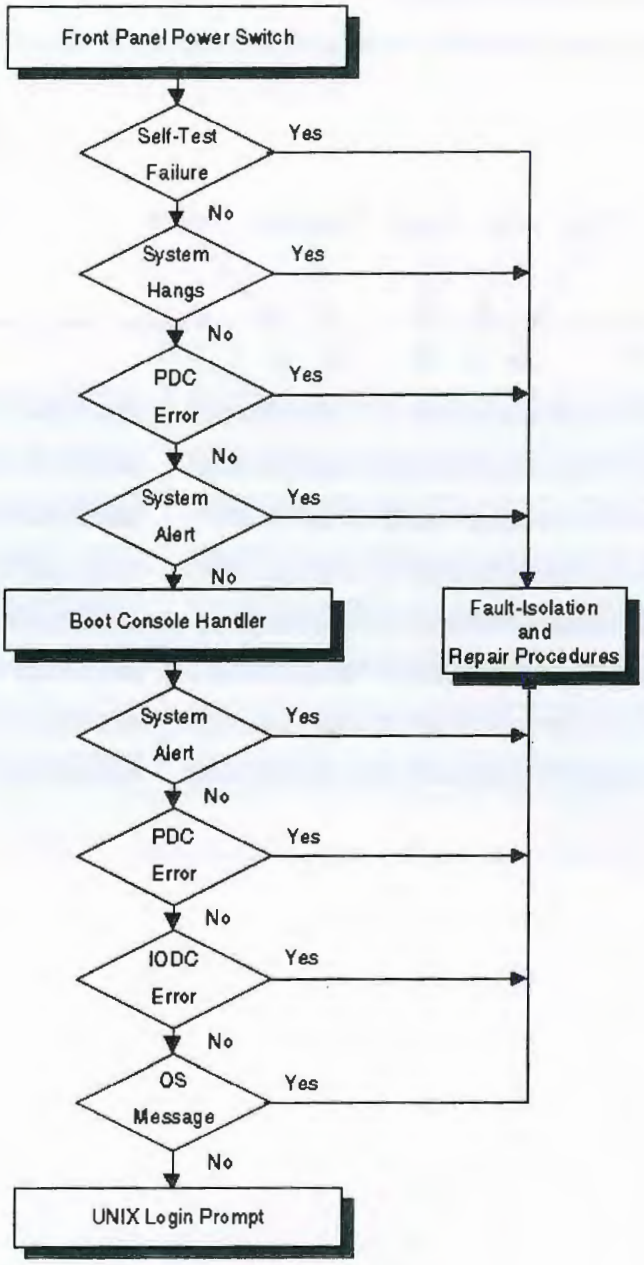
Step 2. Apply power to the rp54xx server by turning the front panel switch to ON.



RQS Nº 03/2005 - CN
CPMI - CORREIOS
0088
Fls:
Doc: 3701

During the Boot process a variety of errors or problems can occur as shown below:

Potential Boot Problems



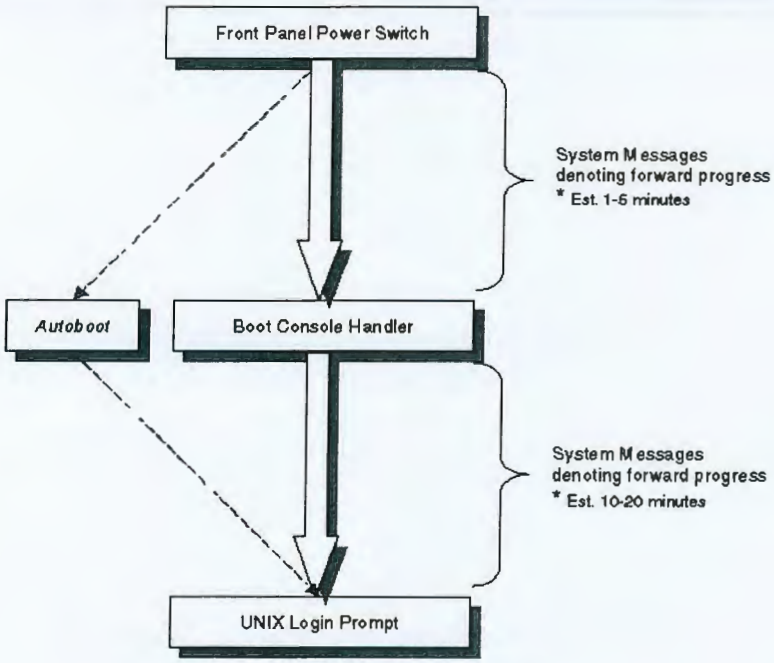
3.094
frente

rp54xx Server Boot Process

The length of time an rp54xx server will require to complete the boot process depends on the number of processors and the amount of RAM installed. Average configurations can take more than 20 minutes.

The boot process consists of the following main steps:

Typical Boot Process



The duration of the full boot process can vary depending on:
- Number of CPUs installed
- Amount of memory installed
- UNIX version installed
- State of the network

All times approximate

IRQS Nº 03/2005 - CN
CORREIOS
0089
Fls:
3701
Doc:

Return the GSP to Default Configurations

The Default Configuration (dc) command is used to reset all or some of the GSP values to the default values. To return GSP values to default configurations, perform the following steps:

1. Access the GSP with the ctrl+b entry.
2. At the GSP prompt, enter the Default Configuration (dc) command:

   ```
   GSP> dc
   ```

3. Follow the prompts for the dc command, and be sure to have the change information available.

CAUTION When the Security configuration is reset, all users are removed, including the GSP administrator. It also disables the remote. Remote must be re-enabled through the main console using the Enable Remote (er) command.

3096
fls

CAUTION Be sure to read each prompt carefully and enter the correct response. A missed or incorrect entry could deny entry to that user.

The following is an example of an added user's information:

```
. User's Name: Joe Smith
. Organization's Name: IT Support
. Dial-back configuration: Disabled
. Access Level: Operator
. Mode: multiple
. User's state: enabled
```

For the number 1 user, the Access level is administrator. The Mode entry of single only allows entry for that user one time, then access will be denied. A Mode entry of multiple allows unlimited entries into the GSP.

Removing Users

You can remove (disable) a GSP user with the same Security options and access control (SO) command used to add user.

To remove a user, perform the following steps:

1. Access the GSP with the ctrl+b entry.
2. At the GSP prompt, enter the Security options and access control (SO) command:

   ```
   GSP> so
   ```

3. The first prompt you will see with the SO command is for GSP-wide parameters:

   ```
   GSP wide parameters are:
   . Login Timeout: 1 minutes.
   . Number of password Faults allowed: 3
   . Flow Control Timeout: 5 minutes.

   Do you want to modify the GSP wide parameters? (Y / [N]) __
   ```

   At this point you can modify the GSP wide parameters, or continue with removing a user. To remove users, respond N for no.

NOTE You will have to step through each user number until you reach the user to be removed.

4. When you access the number of the user to be removed, you must change the data in the prompts for that number.

   It is important that, at a minimum, you need to modify the User's state to Disabled.

ROS Nº 04/2005 - CN
CPMI - CORREIOS
0090
Fls:
3701
Doc:

GSP Configurable Parameters

Once a system console is configured, additional GSP parameters may be set. For a complete list use the GSP>he command to access the on-line help facility.

Examples of three configurable parameters follow.

Adding Users

The GSP provides a maximum of 20 users (one administrator and 19 operators). By design, the first user added to the GSP becomes the GSP administrator. Only the GSP administrator can add or remove users or change the GSP configuration.

NOTE Before starting this procedure, you will need to know the following information:

- User's name
- Organization's name
- Login name
- User's password

To add a user, perform the following steps:

1. Access the GSP with the ctrl+b entry.
2. At the GSP prompt, enter the Security options and access control (SO) command:

   GSP> so
3. The first prompt you will see with the so command is for GSP wide parameters:

```
GSP wide parameters are:
Login Timeout: 1 minutes.
. Number of password Faults allowed: 3
. Flow Control Timeout: 5 minutes.
Do you want to modify the GSP wide parameters? (Y / [N]) __
```

   At this point you can modify the GSP wide parameters, or continue with adding users. To add users, respond N for no.

NOTE If this is the first time users are being added, the first user added will be the GSP administrator.

If this is not the first time you are adding users (you are adding additional users), you will need to step through all current users to reach the next available user prompt.

4. The next prompt that appears will ask the following question:

   Do you want to modify the user number 1 parameters? (Y/[N]/Q to quit) __

   Follow the series of prompts to enter all the required fields for adding a user.

3098

Step 8. Connect the 9-pin end of the RS-232 cable (Supplied) to the connector labeled CONSOLE on the A5591-63002 "W-type" adapter cable.

CAUTION To prevent unauthorized access to your rp54xx system, do not connect the other end of the serial cable to the Secure Web Console until both the server and the Web Console have both been fully configured.

Step 9. Connect one end of a LAN cable to RJ-45 connector labeled 10-Base-T on the Secure Web Console.

Step 10. Connect the other end of the same LAN cable to your site LAN.

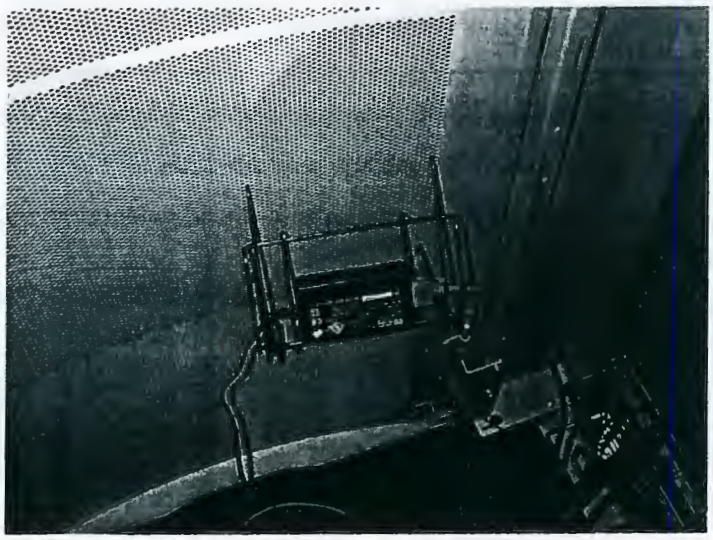
Step 11. Configure the Secure Web Console in accordance with the documentation that was provided with it or refer to http://www.docs.hp.com

Step 12. Once the Web Console has been properly configured, the remaining end of the serial cable between the server and the Web Console may be connected.

ROS Nº 03/2005 - CN
CPMI - CORREIOS
0091
Fls:
3701
Doc:

3.099
Item

Step 2. Place the Secure Web Console power supply into the bottom portion of the wire mounting bracket as shown.



Step 3. Connect one end of the power cable to the power supply where indicated.

Step 4. Position the Secure Web Console unit in the mounting bracket.

Step 5. Connect the DC out cable from the power supply to the Secure Web Console.

Step 6. Connect one end of the AC power cord (supplied) to the Secure Web Console power supply.

Step 7. Connect the other end of the AC power cord to an available receptacle.
On a PDU if in a cabinet.
In an available wall outlet if in a Deskside enclosure.

3100
Front

Secure Web Console Installation

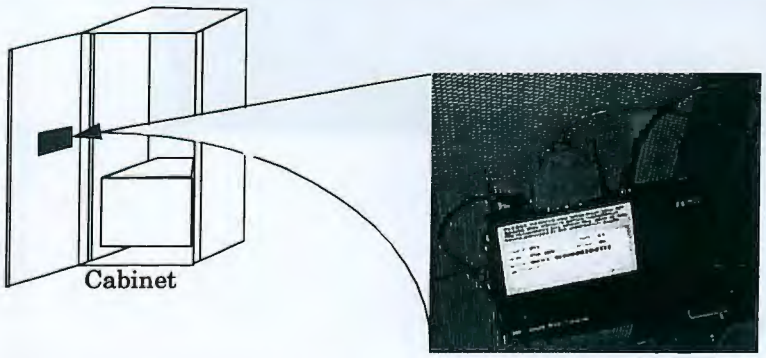
The following section describes installation of the HP Secure Web Console on inside of the rear door of a rack-mounted rp54xx server.

For technical, installation, and configuration instructions for the Secure Web Console, refer to the following URLs on the Internet:

General information:
http://www.hp.com/

Documentation:
http://www.docs.hp.com

NOTE Either the system console (HP series 700 terminal) or the HP Secure Web Console may be installed on an rp54xx server, but not at the same time. Both console types use the same DB9 type LAN *Console* connector.

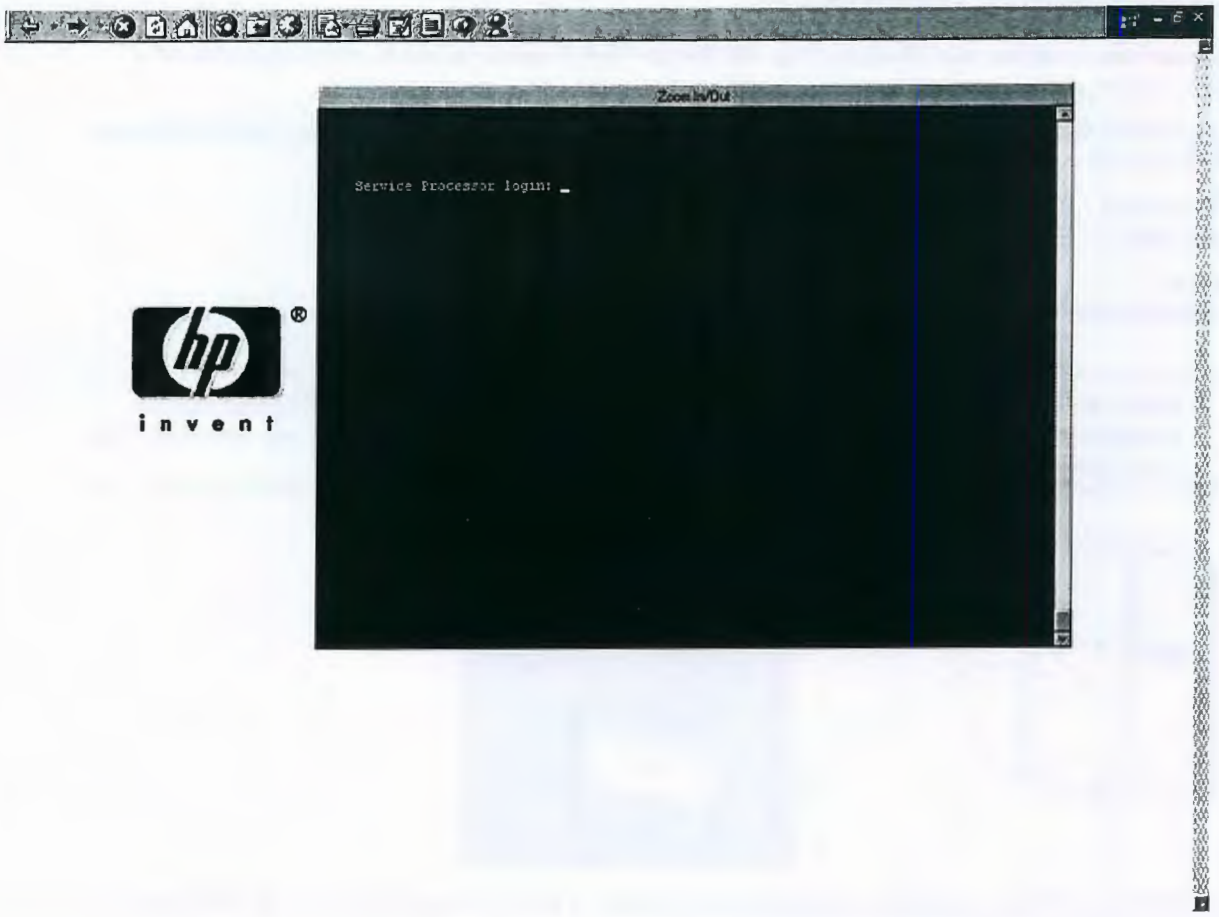


To install the HP Secure Web Console on an rp54xx server, refer to the previous figure and the HP Secure Web Console documentation, then proceed as follows:

Step 1. Install the wire mounting bracket by carefully inserting the two top prongs through the vent grill in the rear door of the cabinet as shown above. Position the bracket toward the hinge side of the door.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 0092
Doc: 3701

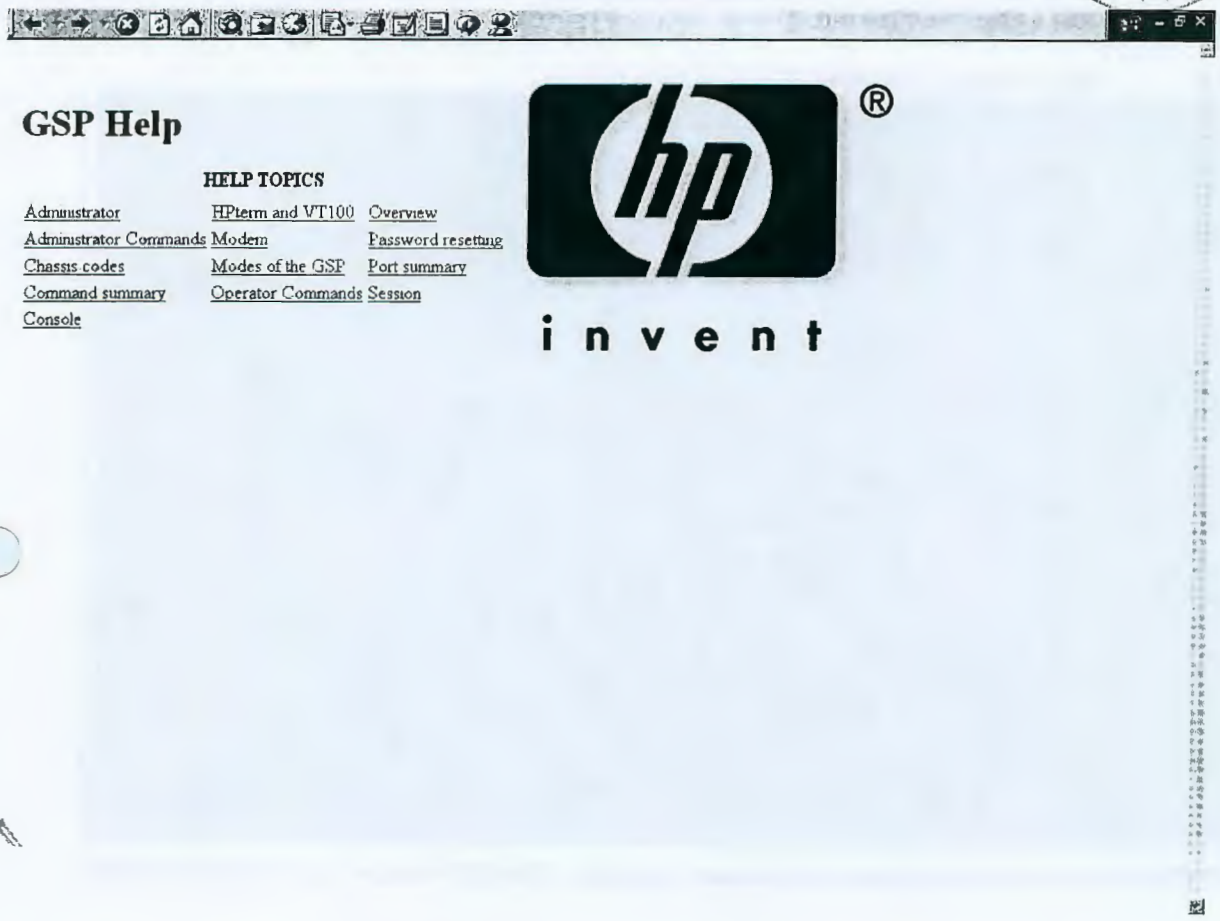
Example 4-6 Combined GSP Browser Window



There is not a separate administration "layer" when using the embedded web access of the revision B GSP. Web console access via the external Secure Web Console required that you first logon to the SWC, then click on ACCESS CONSOLE. User configuration was also performed at the Secure Web Console. However, the revision B GSP web console does not require this additional step. When you point the web browser at the IP of the GSP LAN, you are directly connected to the GSP. The web console part of the GSP employs the same users as the GSP.

3102
Dani

Example 4-5 GSP Web Browser Help Screen



When the separate GSP window is closed, it appears in the HP invent window with Zoom In/Out above it. Click on the Zoom In/Out bar to generate a separate GSP window.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 0093
3701
Doc:

Two browser windows will appear: a window with a white background and the HP invent logo and a separate GSP window with a black background.

Example 4-4 GSP Browser Window

Use the SETTINGS menu bar to configure web browser emulation. The GSP window also has its own HELP facility.

2.998
fls

Platform Monitor Removal

The Platform Monitor resides on the System Board and is accessed via the Top Service Bay.

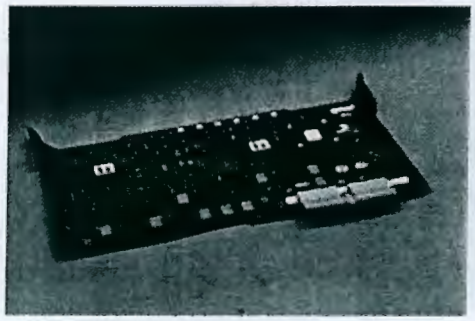
Removing rp5400 and/or rp5450 Model Platform Monitors

Looking into the Top Service Bay from the front, the rp5400/rp5450 model Platform Monitor is located on the left side at the front of the server.

To remove the rp5400/rp5450 model Platform Monitor, perform the following steps:

1. Pull up on the extractor levers on each end of the Platform Monitor to unseat it from its socket.
2. When the Platform Monitor unseats from the socket, pull it up and away from the System Board.

The following graphics show a Platform Monitor board followed by a display of Platform Monitor removal/replacement.



Removing The rp5470 Model Platform Monitor

Looking into the Top Service Bay from the front, the rp5470 model Platform Monitor is located on the right side at the front of the server.

To remove an rp5470 model Platform Monitor, perform the following steps:

1. Pull up on the extractor levers on each end of the Platform Monitor to unseat it from its socket.
2. When the Platform Monitor unseats from the socket, pull it up and away from the System Board.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0094
Fls:
Doc: 3701

Display Board Replacement

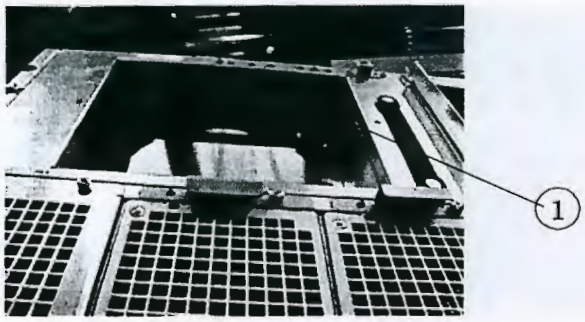
The Display Board contains the server's ON/OFF switch and five LEDs that indicate server status when power is applied.

CAUTION The Display Board is not a HotSwap or HotPlug unit. Ensure that it is powered-down prior to removal.

To replace the Display Board, perform the following tasks:

1. Reconnect the ribbon cable to the Display Board.
2. Carefully push the Display Board up through the top of the Chassis Fan cavity and insert the LEDs and On/Off switch into their respective chassis openings.
3. Replace three T-10 screws.

The following graphic shows the Display Board location (item 1) (looking up from the bottom of the front of the server).



The next graphic shows the Display Board module.

ECT 3.000 Jun

Display Board Removal

The Display Board contains the server's ON/OFF switch and five LEDs that indicate server status when power is applied.

CAUTION The Display Board is not a HotSwap or HotPlug unit. Ensure that the server is powered-down prior to removal.

To remove the Display Board, perform the following tasks:

1. Remove the three T-10 screws that hold the Display Board in place near the top of the chassis front.
2. Remove the two T-15 screws that hold the front Chassis Fan in place and extract the fan from the server.
3. Reach up through the top of the Chassis Fan cavity and carefully pull the Display Board back to free the LEDs and the On/Off switch from their chassis openings. Pull the Display Board down through the Chassis Fan cavity.
4. Disconnect the ribbon cable from the Display Board, and place the display board on a suitable work surface.

The following graphic shows the Display Board access location (item 1) (looking up from the bottom of the front of the server).

The next graphic shows the Display Board module.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 0095
Doc: 3701

Memory DIMM Replacement

Memory DIMMs reside in slots located on the System Board (up to eight). They are loaded in DIMM pairs of equal size.

Replacing rp5400 and/or rp5450 Memory DIMMs

To replace a memory DIMM, perform the following steps:

1. Seat the memory DIMM into its socket.
2. Press the extractor levers on each end of the memory DIMM slot inward until the levers snap into place.

The following graphics show a memory DIMM and a display of DIMM removal/replacement.

Replacing rp5470 Memory DIMMs

To replace an rp5470 memory DIMM, perform the following steps:

1. Seat the memory DIMM into its socket on the Memory Carrier.
2. Press the extractor levers on each end of the memory DIMM slot inward until the levers snap into place.
3. Attach the Memory Clip to the Memory Carrier with the DIMM slot markings on the top of the Memory Clip aligned with the DIMM slot markings on the Memory Carrier. Secure the Memory Clip using the captive screws.
4. Seat the Memory Carrier into the slot on the System Board.
5. Push down on the extractor levers and snap them into place.

3.002 Brent

Memory DIMM Removal

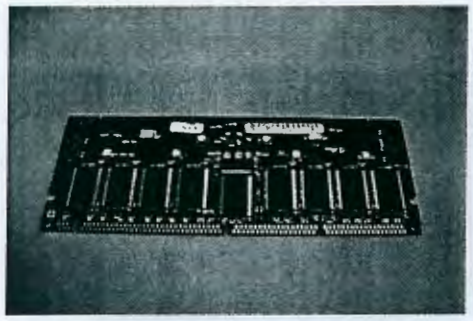
Memory DIMMs reside in slots (up to eight) located on the System Board. They are loaded in DIMM pairs of equal size.

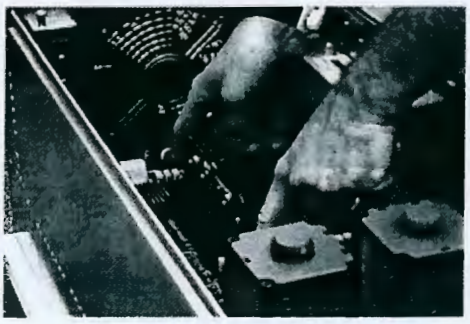
Removing rp5400 Memory DIMMs

To remove an rp5400 memory DIMM, perform the following steps:

1. Press down on the extractor levers on each end of the selected memory DIMM to unseat the DIMM from its socket.
2. When the memory DIMM unseats from the socket, pull it up and away from the System Board.

The following graphics show a memory DIMM, followed by a display of a DIMM being removed/replaced.





emoving rp5470 Memory DIMMs

To remove an rp5470 memory DIMM, perform the following steps:

1. Pull up on the extractor levers on each end of the Memory Carrier to unseat the Memory Carrier from its socket.
2. When the Memory Carrier unseats from the socket, pull it up and away from the System Board.
3. Loosen the captive screws that secure the DIMM Clip and remove DIMM Clip from the Memory Carrier.
4. Press down on the extractor levers on each end of the selected memory DIMM to unseat the DIMM from its socket.
5. When the memory DIMM unseats from the socket, pull it up and away from the Memory Carrier.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0096
Fls:
Doc: 3701

3003

Processor Support Module Replacement

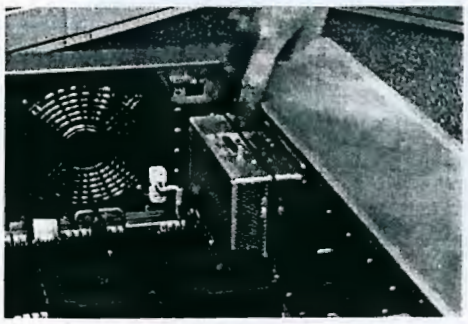
Processor Support Modules (PSMs) (there can be two PSMs, numbered 0 and 1) reside on the System Board and are accessed via the Top Service Bay. Looking into the Top Service Bay from the front, PSMs are located on either side of the server, at the front.

To replace a PSM, perform the following steps:

1. Seat the PSM into its socket.
2. Tighten the two captive mounting screws that hold the PSM in place.

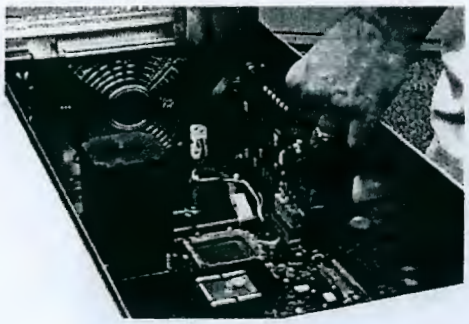
NOTE For the rp5470, the mounting screws have been replaced by posts and the air baffle is used to secure the PSM's.

The following graphic shows a PSM in the server.



2.997 June

The following graphics show a Platform Monitor board followed by a display of Platform Monitor removal/replacement.



RQS Nº 03/2005 - CN
CPMI - CORREIOS
169
Fls: 0097
Doc: 3701

2.996 June

Platform Monitor Replacement

The Platform Monitor resides on the System Board and is accessed via the Top Service Bay.

Replacing rp5400 and/or rp5450 Platform Monitors

Looking into the Top Service Bay from the front, the rp5400/rp5450 model Platform Monitor is located on the left side at the front of the server.

To replace a Platform Monitor, perform the following steps:

1. Seat the Platform Monitor into its socket.
2. Lift the extractor levers and press them onto each end of the Platform Monitor until the levers snap into place.

The following graphics show a Platform Monitor board followed by a display of Platform Monitor removal/replacement.

Replacing rp5470 Platform Monitor

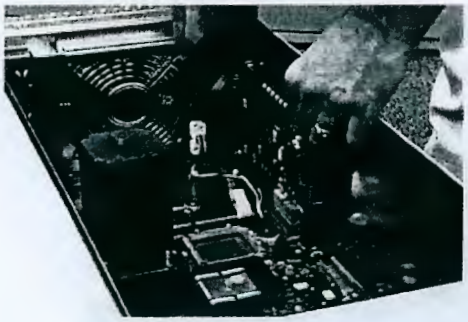
Looking into the Top Service Bay from the front, the rp5470 model Platform Monitor is located on the right side at the front of the server.

To replace a Platform Monitor, perform the following steps:

1. Seat the Platform Monitor into its socket.
2. Lift the extractor levers and press them onto each end of the Platform Monitor until the levers snap into place.

2.995
fls

The following graphics show a Platform Monitor board followed by a display of Platform Monitor removal/replacement.



RQS Nº 03/2005 - CN
CPMI - CORREIOS
0098
Fls:
3701
Doc:

2.994
Irene

PCI I/O Card Removal

The side service bay contains card slots for ten PCI I/O cards (slots 3 through 12) and two Core I/O cards (slots 1 and 2).

Perform the following tasks prior to removing PCI I/O cards:

- Power down the server.
- Detach all power cords from the server.

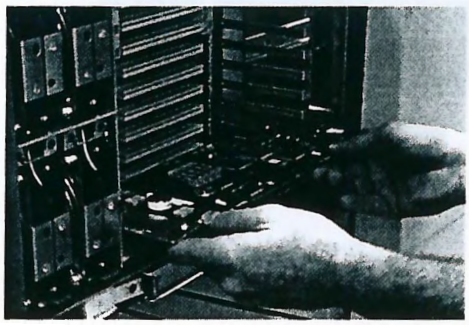
To remove a PCI I/O card from the server, perform the following steps:

NOTE Record the location of all PCI cards as they are removed. Replacing them in a diffferent location will require system reconfiguration and could cause boot failure.

---

1. Disconnect the I/O cable attached to the I/O card at the rear PCI bulkhead.
2. Disconnect any ribbon cable connectors attached to the I/O card in the side service bay.
3. Grasp the edge of the I/O card and pull it out of the server.

The following graphic shows an I/O card being removed.



2.993 June CPL-AS

PCI I/O Card Replacement

The side service bay contains card slots for 10 PCI I/O cards (slots 3 through 12) and 2 Core I/O cards (slots 1 and 2).

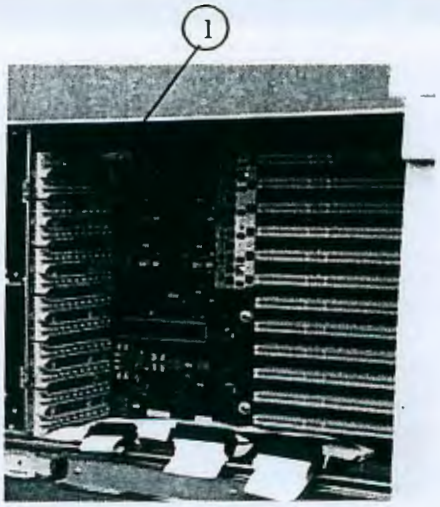
Prior to replacing PCI cards, perform the steps listed below:

- Power down the server.
- Detach all power cords from the server.

To replace a Core or PCI I/O card, perform the following steps:

1. Locate the I/O card guide (item 1) on the outside of the Fan Assembly Housing. Orient the I/O card into its guide slot and push it into the server until the card connector seats in the I/O Backplane card connector.

NOTE Each I/O card guide contains two slots. The top slot is aligned with the I/O Backplane card connector.



2. Connect the I/O cable attached to the I/O card at the rear PCI bulkhead.
3. Connect any ribbon cable connectors attached to the I/O card in the side service bay.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0099
Fls: 173
3701
Doc:

2.992
Irene

The following graphic shows an I/O card being replaced.

E.C.T.
2.991
Irene

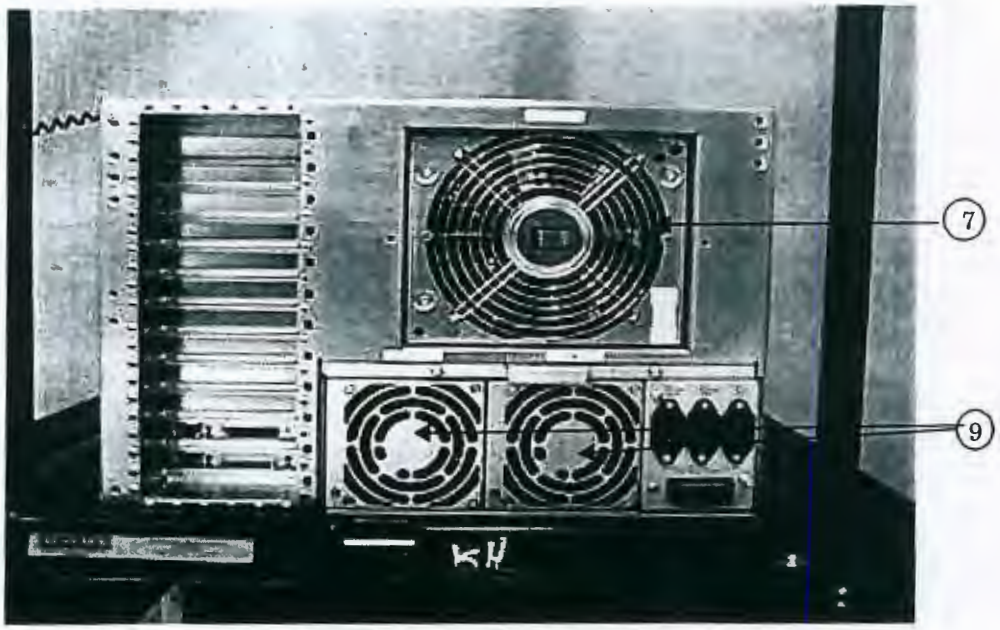
A Parts and Accessories

RQS Nº 03/2005 - CN
CPMI - CORREIOS
175
Fls: 0100
Doc: 3701

CRU Physical Location

This section contains views of the rp54xx computer. The locator numbers in the diagrams correspond to the numbers in the CRU Part Number section.

Figure A-1 Server Rear View



2.989

Figure A-2 Side Service Bay

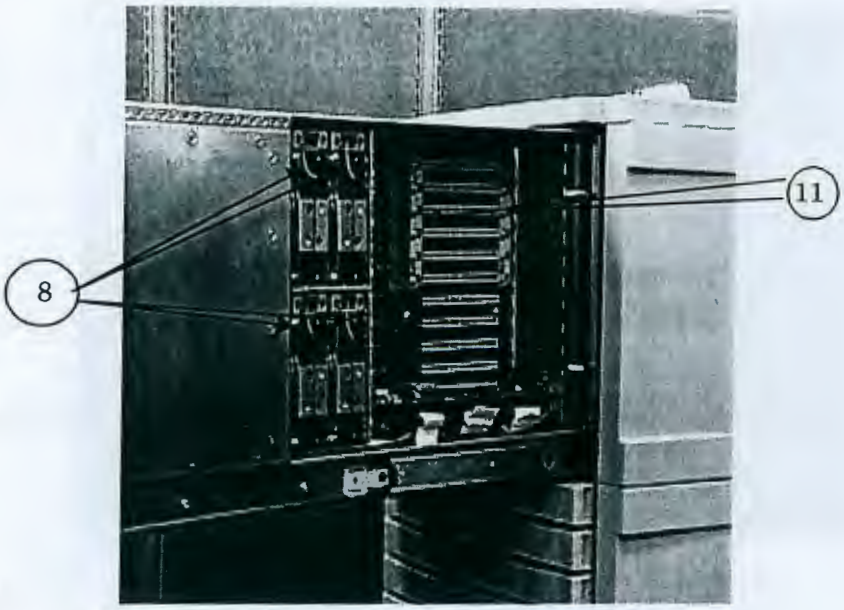
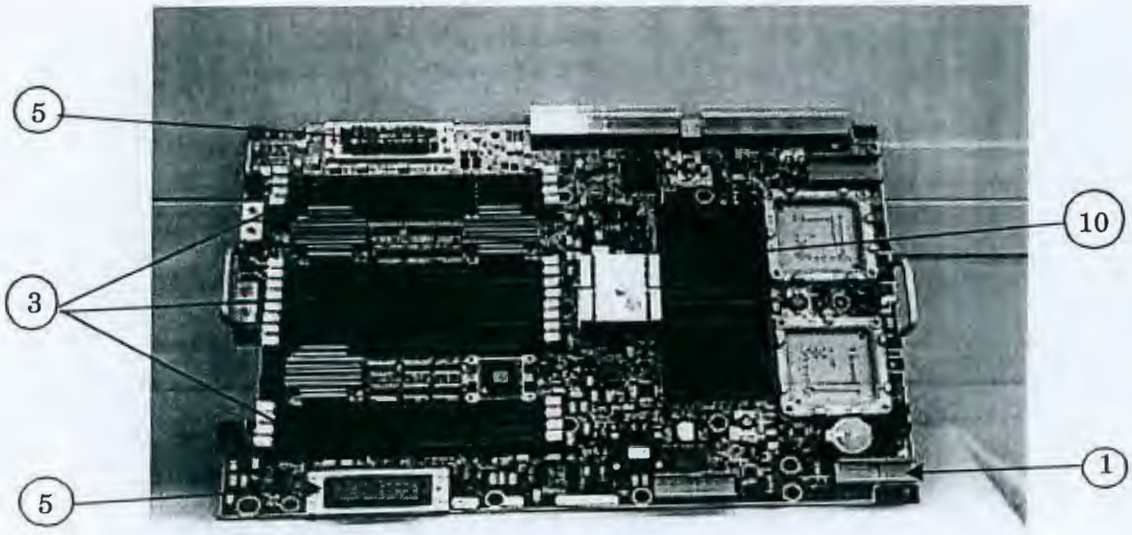


Figure A-3 System Board (Access via Top Service Bay)



ROS Nº 03/2005 - CN
CPMI - CORREIOS
0101
Fls:
Doc: 3701

Figure A-4 Server Front

*The Display Board is accessed by removing the Chassis Fan screen and fan (item 7). The Display Board is located through a slot in the inside top of the Chassis Fan cavity.

2.987
fund

Customer Replaceable Unit Part Numbers

The following tables list all Customer Replaceable Units (CRUs) for the rp54xx computer system. The following tables list both new and exchange part numbers.

Table A-1 Exchange CRUs

Product #	New Part #	Exch. Part #	Description	Loc #
A5191A/B A5576A/B A6144A/B A6797B	A5191-60010	A5191-69010	Platform Monitor Board	1
A5527A	0950-3471	A5527-69001	Power Supply	2
A6155A	A6155-60001	A6155-69001	Memory Carrier	NA
A6115A	A6115-60001	A6115-69001	1024 MB Memory DIMM	3
A5798A	A5798-60001	A5798-69001	512 MB Memory DIMM	
A5797A	A5797-60001	A5797-69001	256 MB Memory DIMM	
A5554A	A5554-60002	A5554-69002	128 MB Memory DIMM	
A5802A	A5802-67001	A5802-69001	9 GB HotPlug Disk Assembly	4
A5803A	A5803-67001	A5803-69001	18 GB HotPlug Disk Assembly	
A6110A	A6110-67001	A6110-69001	36 GB HotPlug Disk Assembly	
A5796A	A3639-60012	A3639-69012	PA-8500/8600 Processor Support Module	5
A6799A	0950-3908	A3639-69033	PA-8700 Processor Support Module	5
A6696A	A5191-60012	A5191-69012	Revision A GSP	NA
A6696B	A6144-60012	A6144-69012	Revision B GSP	NA

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0102
Fls: 3701
Doc:

12.986 June

Table A-2 Non-Exchange CRUs

Product #	Part #	Description	Loc #
A5191A/B A5576A/B A6144A/B A6797B	A5191-60013	Display Board	6
	A5191-04002	Fan, Chassis (172m)	7
	A5191-04003	Fan, Card Cage (119m)	8
	A5191-67006	Fan, Power Converter	9
	0515-0664	Processor Cover Plate	10
	A5236-40024	Disk Filler Panel	NA
	A5191-00107	Power Supply Filler Panel	NA
	A3639-04024	PCI Separator/Extractor	11
A5576A/B A5191A/B A6144A	A5191-04008	Plastic Front Bezel, old style (split door)	NA
A5576A/B A5191A/B A6144A/B	A5191-04012[a]	Plastic Front Bezel, new style rp54xx (solid piece)	NA
A6797B	A5191-04013[a]	Plastic Front Bezel, rp54xx (solid piece)	NA
A5576A/B A5191A/B A6144A/B A6797B	A5191-70010	Bezel Hardware Kit	NA
A6696A	A5191-63001	W-Cable (beige color), use with revision A GSP (A5191-60012/69012) only	NA
A6696B	A6144-63001	M-Cable (black color), use with revision B GSP (A6144-60012/69012) only	NA

a. When replacing the split door bezel (A5191-04008) with a solid piece bezel, the Bezel Hardware Kit (A5191-70010) is required.

E C T
2.985
bune
CPI - AC

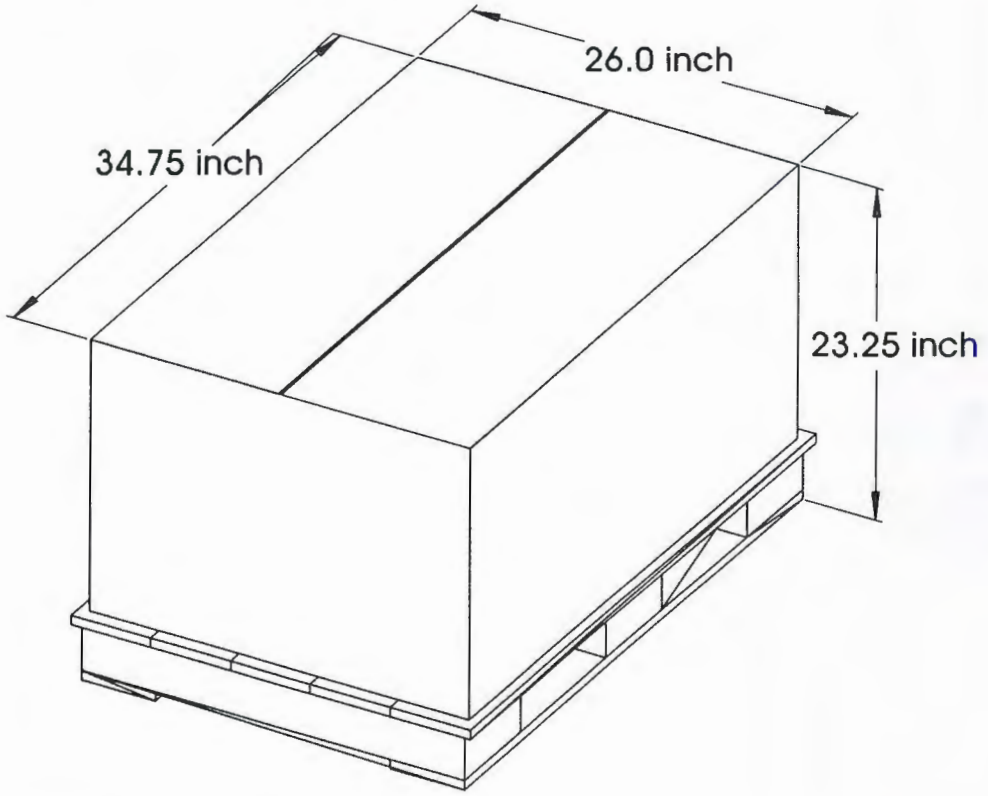
B System Specifications

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0103
Fls:
3701
Doc:

Dimensions

Uncrating Space

rp54xx systems are shipped in boxes on a 34.75 in. x 26 in. (88.25 cm. x 66 cm.) pallet. The combined height of the packaged container and the pallets is 23.25 in. (59 cm.).



rhrr004

Allow a circular area approximately 5 ft. (2 m.) in diameter room for uncrating the system. Allow additional space for temporary storage of the shipping containers and packing materials.

Space Requirements

A minimum access area of 2 ft. (0.7 m.) in all directions is required for serviceability.

2.983
Irene

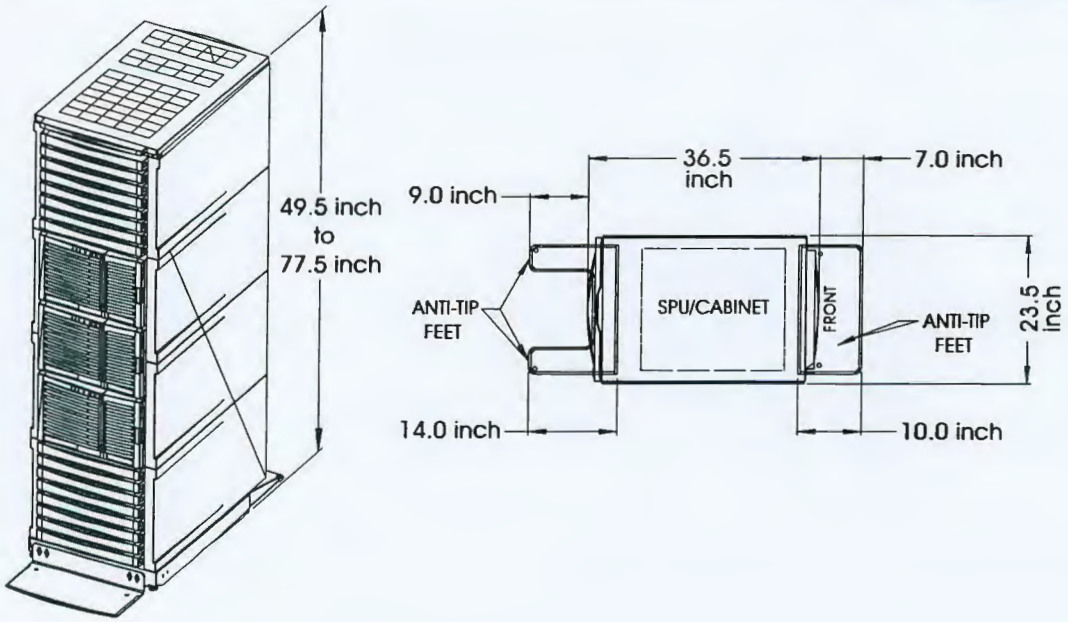
Computer Room Physical Space Requirements

Server

The A5537A, A5538A, or A5539A cabinets in which the server resides is 38.5" deep by 23.5" wide, with heights as follows:

- A5537A 1.2 meter rack - 49.5"
- A5538A 1.6 meter rack - 63.5"
- A5539A 2.0 meter rack - 77.5"

The cabinet anti-tip feet (required for safety) extend the depth an additional 10" in the front and 14" in the back. The minimum standalone physical space for the rp54xx server in a cabinet is shown in the following illustration:



rhrr005

For service access, the server slides on rails 28" beyond the edge of the chassis in the front. An additional minimum of 3' of workspace on all sides is required for servicing the server.

Aisle Space

The minimum aisle space between rows of installed HP rp54xx server/cabinets is 3 feet, front and back, for airflow and serviceability.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0104
Fls:
3701
Doc:

Computer Room Unpacking Space

Specify Uncrating Space

rp54xx Systems are shipped in integrated cabinets on a 34.75" (88.25 cm.) x 26" (66 cm.) pallet. The combined height of the packaged container and the pallets are as follows:

- 1.1 meter rack - 60 inches
- 1.6 meter rack - 73 inches
- 2.0 meter rack - 87 inches

Allow room (a circular area approximately 12 feet (3.5 meters) in diameter) for uncrating the system and rolling the cabinet off the pallet on rails. Allow additional space for temporary storage of the shipping containers and packing materials..

2.981

Electrical

The HP rp54xx power system is comprised of one, two or three autoranging, 12A/10A/5A, 930W hot-swappable system power supplies, depending on how the system is configured. The maximum power needed by fully-configured server is 1200W. Each power supply requires a dedicated 20A branch circuit.

CAUTION HP does not recommend and does not support the use of "ferro-active" or "ferro-resonant" power correction in conjunction with the rp54xx server. These type of line conditioners represent an older technology that is not compatible with the most recent designs in active PFC power supplies such as those in the HP rp54xx servers. "Ferro-active" or "ferro-resonant" line conditioners may cause an increase in total harmonic distortion and may produce significant and unpredictable voltage regulation anomalies.

Office High Availability Requirements

Server-level Enhanced Power Availability

At the server level, enhanced power availability is achieved through the n+1 hot-swappable power supplies.

One power supply is required for a minimally configured rp54xx system operation and in order to allow the system to boot. If a second power supply is present, one of the two power supplies can fail without the system shutting down. Similarly, two power supplies are required for a more heavily-configured rp54xx server. If a third power supply is present, one of the two power supplies can fail without the system shutting down.

If a third (redundant) power supply is present, all three power supplies become hot-swappable. Any one of the power supplies can fail without affecting system performance, and can be replaced while the system is on-line. Single point of failure is reduced to the local wall circuit or PowerTrust UPS to which the power supply power cords are connected.

Power Protection

Power protection is provided through the use of HP PowerTrust UPSs (Uninterruptible Power Supplies). The only supported models for rp54xx systems are the 3.0kVA and 5.5kVA models. Recommendations for other manufacturers and models are not yet determined.

HP rp54xx server power supplies may be plugged directly into the customer's site UPS. However, customers are advised against plugging the power supply into an HP PowerTrust UPS and then connecting that UPS to the site UPS.

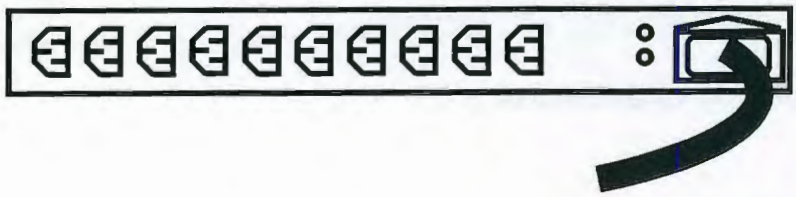
RQS Nº 03/2005 - CN
CPMI - CORREIOS
0105
Fls:
3701
Doc:

Modular PDUs

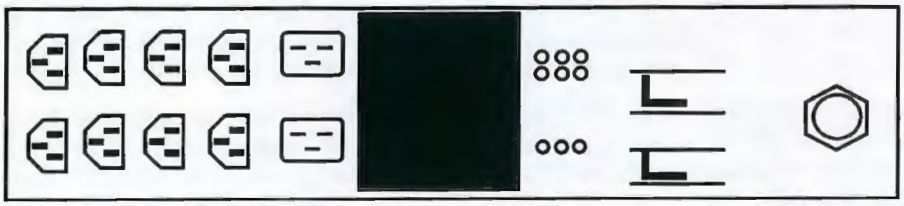
NOTE The acronym PDU (Power Distribution Unit) in this document refers to the power strips attached to the HP rp54xx cabinet.

Three modular PDUs are available for use with the rp54xx product:

- 20A modular PDU, HP product number E7674A. This PDU has seven C13 outlets and one C19 outlet. Note that if this PDU is used to power the rp54xx server, any other peripherals must have their power supplied by additional PDUs in the cabinet. The PDU power cord (HP part number 8120-6903) has an L6-20P plug which must be plugged into an L6-20R wall or floor receptacle.



- 30A modular PDU, HP product number E7681A (North America) or E7682A (International). This PDU has eight C13 outlets and two C19 outlets, split across two 20A branch circuits (max. 30A available). The PDU power cord has an L6-30 plug.



- 60A modular PDU, HP product number E7683A (North America) or E7667A (International). FINAL DESIGN ON THIS PRODUCT IS NOT YET AVAILABLE.

System Power Requirements

Table B-1 Power Requirements

Requirements	Value	Comments
Nominal input voltage	100-240 VAC	
Frequency range (minimum - maximum)	50 - 60 HZ	
Number of phases	1	
Theoretical maximum current	12.0 A	Per line cord
Maximum inrush current	69.0 A	Per line cord
Ground leakage current (mA)	< 3.6 mA	Per line cord

2.979
bene

LAN and Telephone

rp54xx servers provide remote console access via the secure web console, which may be connected to the RS-232 serial port or 10Base-T RJ45 LAN port on the GSP (Guardian Service Processor) card in I/O slot #2. The same connectors may also be used to connect directly to a hard console.

NOTE The RJ45 LAN port should be used ONLY for remote console access and not as a production LAN port.

rp54xx servers may require as many as three unique IP addresses:

- The rp54xx server requires its own IP address.
- The Guardian Service Processor, as a separate network device, has to have its own IP address, gateway, and subnet mask configured at the site in order to be separately addressed. The service processor does not support DHCP, so the IP address must be assigned out of a separate pool from any that are assigned dynamically.
- The remote web console, if used, requires its own IP address.

NOTE Check with your local telephone company to be thatsure the telephone service at the site can accommodate modem/data quality transmission.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
187
0106
Fls:
Doc: 3701

Acoustic Safety Standards

The acoustic specifications for the rp54xx server are as follows:

Sound power	7.0 Bels LwA maximum at >31° C
Sound pressure	60 dB maximum at > 31° C
	No prominent tones

2.975
fls

Altitude Operation Standards

Maximum Altitude	
Operational	3000 meters above sea level
Non-operational	4572 meters above sea level

Effects of Altitude

Some old models of tape drives, including those supplied by Hewlett-Packard, have vacuum column transport mechanisms that are affected by atmospheric pressure. Adjustments to these mechanisms may be required to compensate for the lower atmospheric pressure at higher altitudes.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 0107
Doc: 3701

Temperature and Humidity Operating Standards

The following table lists the temperature and humidity specifications for rp54xx servers.

Temperature and Humidity Specifications				
Parameter	**Operational Limits**	**Recommended Operating Range**	**Maximum Rate of Change (per hour)**	**Non-Operating Ranges**
Temperature[a]	5°C to 35°C (41°F to 95°F)[b]	20°C to 25°C (68°F to 77°F)	10°C (50°F) per hour (With tape media) 20°C (68°F) per hour (Without tape media)	-40°C to +70°C (-40°F to +158°F)
Operating Humidity	15 to 80% Relative humidity (Non-condensing) at 35°C (95°F)	40 to 60% Relative humidity (Non-condensing)	30% Per hour Relative humidity (Non-condensing)	90% Relative humidity (Non-condensing) at 65°C (149°F)

a. The rp54xx has been designed to operate within the above specific temperature and relative humidity operational limits. In general, operating any electronic equipment within the recommended ranges of temperature and humidity will produce optimal reliability.

b. Temperature ranges stated above are at sea level. Maximum operating temperature is derated (reduced) by 2°C for each 1000 meters above sea level up to a maximum of 3000 meters.

NOTE Operating ranges refer to the ambient air temperature and humidity measured at the cabinet cooling air intake vents.

Thermal Protection Features

If the cabinet temperature approaches 35°C, thermal protection will be invoked. At 35°C +/- 2°C a warning message will be displayed on the system console. At 40°C +/- 2°C an ungraceful shutdown will occur.

2.973
bene

C General Site Preparation Guidelines

The following information provides general principles and practices to consider before the installation or operation of an hp server.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0108
Fls:
3701
Doc:

Electrical Factors

Proper design and installation of a power distribution system for an hp server requires specialized skills. Those responsible for this task must have a thorough knowledge and understanding of appropriate electrical codes and the limitations of the power systems for computer and data processing equipment.

In general, a well-designed power distribution system exceeds the requirements of most electrical codes. A good design, when coupled with proper installation practices, produces the most trouble-free operation.

A detailed discussion of power distribution system design and installation is beyond the scope of this information. However, electrical factors relating to power distribution system design and installation must be considered during the site preparation process.

The electrical factors discussed in this section are:

- Computer room safety
- Power Consumption
- Electrical load requirements (circuit breaker sizing)
- Power quality
- Distribution hardware
- System installation guidelines

Computer Room Safety

Inside the computer room, fire protection and adequate lighting (for equipment servicing) are important safety considerations. Federal and local safety codes govern computer installations.

Fire Protection

The National Fire Protection Association's Standard for the Protection of Electronic Computer Data Processing Equipment, NFPA 75, contains information on safety monitoring equipment for computer rooms.

Most computer room installations are equipped with the following fire protection devices:

- Smoke detectors
- Fire and temperature alarms
- Fire extinguishing system

Additional safety devices are:

- Circuit breakers
- An emergency power cutoff switch
- Devices specific to the geographic location i.e., earthquake protection

Lighting Requirements for Equipment Servicing

Adequate lighting and utility outlets in a computer room reduce the possibility of accidents during equipment servicing. Safer servicing is also more efficient and, therefore, less costly.

For example, adequate lighting reduces the chances of connector damage when cables are installed or removed.

2.971
Jun

The minimum recommended illumination level is 70 foot-candles (756 lumens per square meter) when the light level is measured at 30 inches (76.2 cm) above the floor.

Power Consumption

When determining power requirements, you must consider any peripheral equipment that will be installed during initial installation or as a later update. Refer to the applicable documentation for such devices to determine the power required to support these devices.

Electrical Load Requirements (Circuit Breaker Sizing)

NOTE Local authority has jurisdiction [LAHJ] and should make the final decision regarding adherence to country- specific electrical codes and guidelines.

It is good practice to derate power distribution systems for one or more of the following reasons:

To avoid nuisance tripping from load shifts or power transients, circuit protection devices should never be run above 80% of their root-mean-square (RMS) current ratings.

- Safety agencies derate most power connectors to 80% of their RMS current ratings.

Power Quality

The hp server is designed to operate over a wide range of voltages and frequencies. The server is tested and shown to comply with EMC Specification EN50082. However, damage can occur if these ranges are exceeded. Severe electrical disturbances can exceed the design specifications of the equipment.

Sources of Voltage Fluctuations

Voltage fluctuations, sometimes called glitches, affect the quality of electrical power. Common sources of these disturbances are:

- Fluctuations occurring within the facility's distribution system
- Utility service low-voltage conditions (such as sags or brownouts)
- Wide and rapid variations in input voltage levels
- Wide and rapid variations in input power frequency

Electrical storms

- Large inductive sources (such as motors and welders)
- Faults in the distribution system wiring (such as loose connections)
- Microwave, radar, radio, or cell phone transmissions

RQS Nº 0082005 - CN
CPMI - CORREIOS
0109
Fls:
Doc: 3701

Power System Protection

The hp server can be protected from the sources of many of these electrical disturbances by using:

- A dedicated power distribution system
- Power conditioning equipment
- Over- and under-voltage detection and protection circuits
- Screening to cancel out the effects of undesirable transmissions
- Lightning arresters on power cables to protect equipment against electrical storms

Precautions have been taken during power distribution system design to provide immunity to power outages of less than one cycle. However, testing cannot conclusively rule out loss of service. Therefore, adherence to the following guidelines provides the best possible performance of power distribution systems for hp computer equipment:

- Dedicated power source—Isolates an hp server power distribution system from other circuits in the facility.
- Missing-phase and low-voltage detectors—Shuts equipment down automatically when a severe power disruption occurs. For peripheral equipment, these devices are recommended but optional.
- Online uninterruptible power supply (UPS)—Keeps input voltage to devices constant and should be considered if outages of one-half cycle or more are common. Refer to qualified contractors or consultants for each situation.

Distribution Hardware

This section describes wire selection and the types of raceways (electrical conduits) used in the distribution system.

Wire Selection

Use copper conductors instead of aluminum, as aluminum's coefficient of expansion differs significantly from that of other metals used in power hardware. Because of this difference, aluminum conductors can cause connector hardware to work loose, overheat, and fail.

Raceway Systems (electrical conduits) [LAHJ]

Raceways (electrical conduits) form part of the protective ground path for personnel and equipment. Raceways protect the wiring from accidental damage and also provide a heatsink for the wires.

Any of the following types may be used:

- Electrical metallic tubing (EMT) thin-wall tubing
- Rigid (metal) conduit
- Liquidtight with RFI shield grounded (most commonly used under raised floors)

Building Distribution

All building feeders and branch circuitry should be in rigid metallic conduit with proper connectors (to provide ground continuity) Conduit that is exposed and subject to damage should be constructed of rigid galvanized steel.

2.969
Fls.

Grounding Systems

An hp server requires two methods of grounding:

- Power distribution safety grounding
- High frequency intercabinet grounding

Power Distribution Safety Grounding [LAHJ]

The power distribution safety grounding system consists of connecting various points in the power distribution system to earth ground using green (green/yellow) wire ground conductors. Having these ground connections tied to metal chassis parts that may be touched by computer room personnel protects them against shock hazard from current leakage and fault conditions.

Power distribution systems consist of several parts. Hewlett-Packard recommends that these parts be solidly interconnected to provide an equipotential ground to all points.

Main Building Electrical Ground The main electrical service entrance equipment should have an earth ground connection, as required by applicable codes. Connections such as a grounding rod, building steel, or a conductive type cold water service pipe provide an earth ground.

Electrical Conduit Ground All electrical conduits should be made of rigid metallic conduit that is securely connected together or bonded to panels and electrical boxes, so as to provide a continuous grounding system.

Power Panel Ground Each power panel should be grounded to the electrical service entrance with green (green/yellow) wire ground conductors. The green (green/yellow) wire ground conductors should be sized per applicable codes (based on circuit over current device ratings).

NOTE The green wire ground conductor mentioned above may be a black wire marked with green tape. [LAHJ]

Computer Safety Ground Ground all computer equipment with the green (green/yellow) wire included in the branch circuitry. The green (green/yellow) wire ground conductors should be connected to the appropriate power panel and should be sized per applicable codes (based on circuit over current device ratings).

Cabinet Performance Grounding (High Frequency Ground)

Signal interconnects between system cabinets require high frequency ground return paths. Connect all cabinets to site ground.

NOTE In some cases power distribution system green (green/yellow) wire ground conductors are too long and inductive to provide adequate high frequency ground return paths. Therefore, a ground strap (customer-supplied) should be used for connecting the system cabinet to the site grounding grid (customer-supplied). When connecting this ground, ensure that the raised floor is properly grounded for high frequency.

Power panels located in close proximity to the computer equipment should also be connected to the site grounding grid. Methods of providing a sufficiently high frequency ground grid are described in the next sections.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0110
Fls:
Doc: 3701

D. 968 here

Raised Floor "High Frequency Noise" Grounding

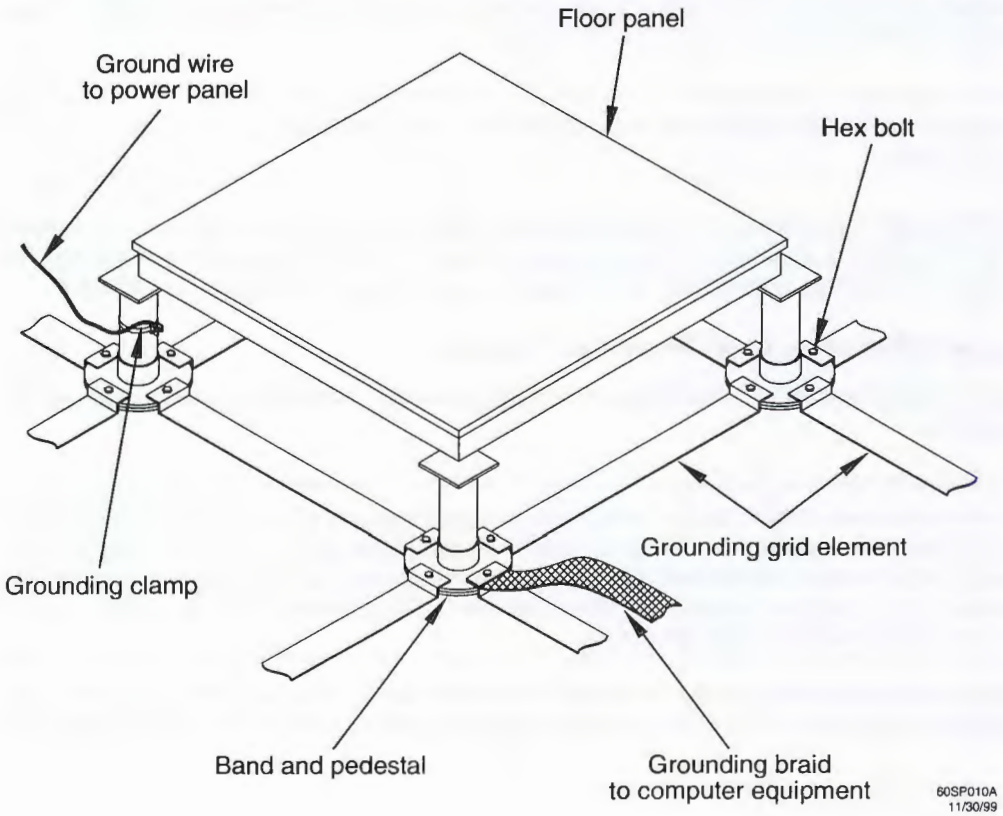
If a raised floor system is used, install a complete signal grounding grid for maintaining equal potential over a broad band of frequencies. The grounding grid should be connected to the equipment cabinet and electrical service entrance ground at multiple connection points using a minimum #6 AWG (16mm2) wire ground conductor. The following figure illustrates a metallic strip grounding system.

Hewlett-Packard recommends the following approaches:

- Excellent—Add a grounding grid to the subfloor. The grounding grid should be made of copper strips mounted to the subfloor. The strips should be 0.032 in. (0.08 cm) thick and a minimum of 3.0 in. (8.0 cm) wide.

  Connect each pedestal to four strips using 1/4 in. (6.0 mm) bolts tightened to the manufacturer's torque recommendation.
- Better - A grounded #6 AWG minimum copper wire grid mechanically clamped to floor pedestals and properly bonded to the building/site ground.
- Good—Use the raised floor structure as a ground grid. In this case, the floor must be designed as a ground grid with bolted down stringers and corrosion resistive plating (to provide low resistance and attachment points for connection to service entrance ground and hp computer equipment). The use of conductive floor tiles with this style of grid further enhances ground performance.

Figure C-1 Raised Floor Metal Strip Ground System



2.967
fls.

Equipment Grounding Implementation Details

Connect all Hewlett-Packard equipment cabinets to the site ground grid as follows:

Step 1. Attach one end of each ground strap to the applicable cabinet ground lug.

Step 2. Attach the other end to the nearest pedestal base (raised floor) or cable trough ground point (nonraised floor).

Step 3. Check that the braid contact on each end of the ground strap consists of a terminal and connection hardware (a 1/4-in. (6.0-mm) bolt, nuts, and washers).

Step 4. Check that the braid contact connection points are free of paint or other insulating material and treated with a contact enhancement compound (similar to Burndy Penetrox).

System Installation Guidelines

This section contains information about installation practices. Some common pitfalls are highlighted. Both power cable and data communications cable installations are discussed.

NOTE In domestic installations, the proper receptacles should be installed prior to the arrival of Hewlett-Packard equipment. Refer to the appropriate installation guide for installation procedures.

Wiring Connections

Expansion and contraction rates vary among different metals. Therefore, the integrity of an electrical connection depends on the restraining force applied. Connections that are too tight compress or deform the hardware and causes it to weaken. This usually leads to high impedance preventing circuit breakers from tripping when needed or can contribute to a buildup of high frequency noise.

CAUTION Connections that are too loose or too tight can have a high impedance that cause serious problems, such as erratic equipment operation. A high impedance connection overheats and sometimes causes fire or high temperatures that can destroy hard-to-replace components such as distribution panels or system bus bars.

Wiring connections must be properly torqued. Many equipment manufacturers specify the proper connection torque values for their hardware.

Ground connections must only be made on a conductive, nonpainted surface. When equipment vibration is present, lock washers must be used on all connections to prevent connection hardware from working loose.

Data Communications Cables

Power transformers create high-energy fields in the form of electromagnetic interference (EMI). Heavy foot traffic can create electrostatic discharge (ESD) that can damage electronic components. Route data communications cables away from these areas. Use shielded data communications cables that meet approved industry standards to reduce the effects of external fields.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0111
Fls:
3701
Doc:

Environmental Elements

The following environmental elements can affect an hp server installation:

- Computer room preparation
- Cooling requirements
- Humidity level
- Air conditioning ducts
- Dust and pollution control
- Electrostatic discharge (ESD) prevention
- Acoustics (noise reduction)

Computer Room Preparation

The following guidelines are recommended when preparing a computer room for an hp server:

- Locate the computer room away from the exterior walls of the building to avoid the heat gain from windows and exterior wall surfaces.
- When exterior windows are unavoidable, use windows that are double or triple glazed and shaded to prevent direct sunlight from entering the computer room.
- Maintain the computer room at a positive pressure relative to surrounding spaces.
- Use a vapor barrier installed around the entire computer room envelope to restrain moisture migration.
- Caulk and vapor seal all pipes and cables that penetrate the envelope.
- Use at least a 12-inch raised floor system for minimum favorable room air distribution system (underfloor distribution).
- Ensure a minimum clearance of 12 inches between the top of the hp server cabinet and the ceiling to allow for return air flow and ensure that all ceiling tiles are in place.
- Allow 18 inches (or local code minimum clearance) from the top of the hp server cabinet to the fire sprinkler heads.

Cooling Requirements

Air conditioning equipment requirements and recommendations are described in the following sections.

Basic Air Conditioning Equipment Requirements

The cooling capacity of the installed air conditioning equipment for the computer room should be sufficient to offset the computer equipment dissipation loads, as well as any space envelope heat gain. This equipment should include:

- Air filtration
- Cooling or dehumidification
- Humidification
- Reheating

ECT 2.965 fls

- Air distribution
- System controls adequate to maintain the computer room within specified operating ranges.

Lighting and personnel must also be included. For example, a person dissipates about 450 BTUs per hour while performing a typical computer room task.

At altitudes above 10,000 feet (3048 m), the lower air density reduces the cooling capability of air conditioning systems. If your facility is located above this altitude, the recommended temperature ranges may need to be modified. For each 1000 feet (305 m) increase in altitude above 10,000 feet (up to a maximum of 15,000 feet), subtract 1.5° F (0.83° C) from the upper limit of the temperature range.

Air Conditioning System Guidelines

The following guidelines are recommended when designing an air conditioning system and selecting the necessary equipment:

- The air conditioning system that serves the computer room should be capable of operating 24 hours a day, 365 days a year. It should also be independent of other systems in the building.
- Consider the long-term value of hp server availability, redundant air conditioning equipment or capacity. The system should be capable of handling any future hp server expansion.
- Air conditioning equipment air filters should have a minimum rating of 45% (based on "ASHRAE Standard 52-76, Dust Spot Efficiency Test").
- Introduce only enough outside air into the system to meet building code requirements (for human occupancy) and to maintain a positive air pressure in the computer room.

Air Conditioning System Types

The following three air conditioning system types are listed in order of preference:

- Complete self-contained package unit(s) with remote condenser(s). These systems are available with up or down discharge and are usually located in the computer room.
- Chilled water package unit with remote chilled water plant. These systems are available with up or down discharge and are usually located in the computer room.
- Central station air handling units with remote refrigeration equipment. These systems are usually located outside the computer room.

Basic Air Distribution Systems

A basic air distribution system includes supply air and return air.

An air distribution system should be zoned to deliver an adequate amount of supply air to the cooling air intake vents of the hp server equipment cabinets. Supply air temperature should be maintained within the following parameters:

- Ceiling supply system—From 55° F (12.8° C) to 60° F (15.6° C)
- Floor supply system—At least 60° F (15.6° C)

If a ceiling plenum return air system or a ducted ceiling return air system is used, the return air grill(s) in the ceiling should be above the exhaust area or the exhaust row.

The following three types of air distribution system are listed in order of recommendation:

- Underfloor air distribution system—Downflow air conditioning equipment located on the raised floor of the computer room uses the cavity beneath the raised floor as plenum for the supply air.

ECT 2.965 fls
ECT Nº 03/2005 - CN
CPMI - CORREIOS
0112
Fls:
Doc: 3701

Perforated floor panels (available from the raised floor manufacturer) should be located around the front of the system cabinets. Supply air emitted though the perforated floor panels is then available near the cooling air intake vents of the hp server cabinets.

- Ceiling plenum air distribution system—Supply air is ducted into the ceiling plenum from upflow air conditioning equipment located in the computer room or from an air handling unit (remote).

  The ceiling construction should resist air leakage. Place perforated ceiling panels (with down discharge air flow characteristics) around the front of the system cabinets. The supply air emitted downward from the perforated ceiling panels is then available near the cooling air intake vents of the hp server cabinets.

  Return air should be ducted back to the air conditioning equipment though the return air duct above the ceiling.

- Above ceiling ducted air distribution system—Supply air is ducted into a ceiling diffuser system from upflow air conditioning equipment located in the computer room or from an air handling unit (remote).

  Adjust the supply air diffuser system grilles to direct the cooling air downward around the front of the hp server cabinets. The supply air is then available near the cooling air intake vents of the hp server cabinets.

Air Conditioning System Installation

All air conditioning equipment, materials, and installation must comply with any applicable construction codes. Installation of the various components of the air conditioning system must also conform to the air conditioning equipment manufacturer's recommendations.

Air Conditioning Ducts

Use separate computer room air conditioning duct work. If it is not separate from the rest of the building, it might be difficult to control cooling and air pressure levels. Duct work seals are important for maintaining a balanced air conditioning system and high static air pressure. Adequate cooling capacity means little if the direction and rate of air flow cannot be controlled because of poor duct sealing. Also, the ducts should not be exposed to warm air, or humidity levels may increase.

Humidity Level

Maintain proper humidity levels at 40 to 60% RH. High humidity causes galvanic actions to occur between some dissimilar metals. This eventually causes a high resistance between connections, leading to equipment failures. High humidity can also have an adverse affect on some magnetic tapes and paper media.

CAUTION Low humidity contributes to undesirably high levels of electrostatic charges. This increases the electrostatic discharge (ESD) voltage potential. ESD can cause component damage during servicing operations. Paper feed problems on high-speed printers are usually encountered in low-humidity environments.

Low humidity levels are often the result of the facility heating system and occur during the cold season. Most heating systems cause air to have a low humidity level, unless the system has a built-in humidifier.

Dust and Pollution Control

Computer equipment can be adversely affected by dust and microscopic particles in the site environment.

Specifically, disk drives, tape drives, and some other mechanical devices can have bearing failures resulting from airborne abrasive particles. Dust may also blanket electronic components like printed circuit boards causing premature failure due to excess heat and/or humidity build up on the boards. Other failures to power

2.963
fls.

supplies and other electronic components can be caused by metallically conductive particles, including zinc whiskers. These metallic particles are conductive and can short circuit electronic components. Use every effort to ensure that the environment is as dust and particulate free as possible. See the following heading titled "Metallic Particulate Contamination" for additional details.

Smaller particles can pass though some filters and over a period of time, cause problems in mechanical parts. Small dust particles can be prevented from entering the computer room by maintaining the air conditioning system at a high static air pressure level.

Other sources of dust, metallic, conductive, abrasive, and/or microscopic particles can be present. Some sources of these particulates are:

- Subfloor shedding
- Raised floor shedding
- Ceiling tile shedding

These particulates are not always visible to the naked eye. A good check to determine their possible presence is to check the underside of the tiles. The tile should be shiny, galvanized, and free from rust.

The computer room should be kept clean. The following guidelines are recommended:

- Smoking—Establish a no-smoking policy. Cigarette smoke particles are eight times larger than the clearance between disk drive read/write heads and the disk surface.
- Printer—Locate printers and paper products in a separate room to eliminate paper particulate problems.
- Eating or drinking—Establish a no-eating or drinking policy. Spilled liquids can cause short circuits in equipment such as keyboards.
- Tile floors—Use a dust-absorbent cloth mop rather than a dry mop to clean tile floors.

Special precautions are necessary if the computer room is near a source of air pollution. Some air pollutants, especially hydrogen sulfide (H2S), are not only unpleasant but corrosive as well. Hydrogen sulfide damages wiring and delicate sound equipment. The use of activated charcoal filters reduces this form of air pollution.

Metallic Particulate Contamination

Metallic particulates can be especially harmful around electronic equipment. This type of contamination may enter the data center environment from a variety of sources, including but not limited to raised floor tiles, worn air conditioning parts, heating ducts, rotor brushes in vacuum cleaners or printer component wear. Because metallic particulates conduct electricity, they have an increased potential for creating short circuits in electronic equipment. This problem is exaggerated by the increasingly dense circuitry of electronic equipment.

Over time, very fine whiskers of pure metal can form on electroplated zinc, cadmium, or tin surfaces. If these whiskers are disturbed, they may break off and become airborne, possibly causing failures or operational interruptions. For over 50 years, the electronics industry has been aware of the relatively rare but possible threat posed by metallic particulate contamination. During recent years, a growing concern has developed in computer rooms where these conductive contaminants are formed on the bottom of some raised floor tiles.

Although this problem is relatively rare, it may be an issue within your computer room. Since metallic contamination can cause permanent or intermittent failures on your electronic equipment, Hewlett-Packard strongly recommends that your site be evaluated for metallic particulate contamination before installation of electronic equipment.

IRQS Nº 03/2005 - CN
CPMI 20 CORREIOS
0113
Fls:
3701
Doc:

C T
2.962
June

Electrostatic Discharge (ESD) Prevention

Static charges (voltage levels) occur when objects are separated or rubbed together. The voltage level of a static charge is determined by the following factors:

- Types of materials
- Relative humidity
- Rate of change or separation

Table C-1 Effect of Humidity on ESD Charge Levels

Personnel Activity[a]	Humidity[b] and Charge Levels (voltages)[c]			
	26%	32%	40%	50%
Person walking across a linoleum floor	**6,150 V**	**5,750 V**	**4,625 V**	**3,700 V**
Person walking across a carpeted floor	18,450 V	17,250 V	13,875 V	11,100 V
Person getting up from a plastic chair	24,600 V	23,000 V	18,500 V	14,800 V

a. Source: B.A. Unger, Electrostatic Discharge Failures of Semiconductor Devices (Bell Laboratories, 1981)
b. For the same relative humidity level, a high rate of airflow produces higher static charges than a low airflow rate.
c. Some data in this table has been extrapolated.

Static Protection Measures

Follow these precautions to minimize possible ESD-induced failures in the computer room:

- Maintain recommended humidity level and airflow rates in the computer room.
- Install conductive flooring (conductive adhesive must be used when laying tiles).
- Use conductive wax if waxed floors are necessary.
- Ensure that all equipment and flooring are properly grounded and are at the same ground potential.
- Use conductive tables and chairs.
- Use a grounded wrist strap (or other grounding method) when handling circuit boards.
- Store spare electronic modules in antistatic containers.

Acoustics

Computer equipment and air conditioning blowers cause computer rooms to be noisy. Ambient noise level in a computer room can be reduced as follows:

- Dropped ceiling—Cover with a commercial grade of fire-resistant, acoustic rated, fiberglass ceiling tile.
- Sound deadening—Cover the walls with curtains or other sound deadening material.
- Removable partitions—Use foam rubber models for most effectiveness.

2.961
fls

Facility Characteristics

This section contains information about facility characteristics that must be considered for the installation or operation of an hp server. Facility characteristics are:

- Floor loading
- Windows
- Altitude effects

Floor Loading

The computer room floor must be able to support the total weight of the installed hp server as well as the weight of the individual cabinets as they are moved into position.

Floor loading is usually not an issue in nonraised floor installations. The information presented in this section is directed toward raised floor installations.

NOTE An appropriate floor system consultant should verify any floor system under consideration for an hp server installation.

Raised Floor Loading

Raised floor loading is a function of the manufacturer's load specification and the positioning of the equipment relative to the raised floor grid. While Hewlett-Packard cannot assume responsibility for determining the suitability of a particular raised floor system, it does provide information and illustrations for the customer or local agencies to determine installation requirements.

The following guidelines are recommended:

- Because many raised floor systems do not have grid stringers between floor stands, the lateral support for the floor stands depends on adjacent panels being in place. To avoid compromising this type of floor system while gaining under floor access, remove only one floor panel at a time.
- Larger floor grids (bigger panels) are generally rated for lighter loads.

CAUTION Do not position or install any equipment cabinets on the raised floor system until you have carefully examined it to verify that it is adequate to support the appropriate installation.

Floor Loading Terms

Table C-2 Floor Loading Term Definitions

Term	Definition
Dead load	The weight of the raised panel floor system, including the understructure. Expressed in lb/ft2 (kg/m2).
Live load	The load that the floor system can safely support. Expressed in lb/ft2 (kg/m2).

RDS Nº 03/2005 - CN
CPMI - CORREIOS
0114
Fls:
Doc: 3701

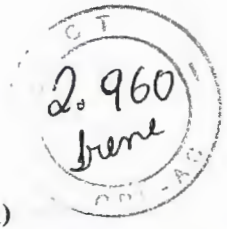


Table C-2 Floor Loading Term Definitions (Continued)

Term	Definition
Concentrated load	The load that a floor panel can support on a 1-in2 (6.45 cm2) area at the panel's weakest point (typically the center of the panel), without the surface of the panel deflecting more than a predetermined amount.
Ultimate load	The maximum load (per floor panel) that the floor system can support without failure. Failure expressed by floor panel(s) breaking or bending. Ultimate load is usually stated as load per floor panel.
Rolling load	The load a floor panel can support (without failure) when a wheel of specified diameter and width is rolled across the panel.
Average floor load	Computed by dividing total equipment weight by the area of its footprint. This value is expressed in lb/ft2 (kg/m2).

Average Floor Loading

The average floor load value is not appropriate for addressing raised floor ratings at the floor grid spacing level. However, it is useful for determining floor loading at the building level, such as the area of solid floor or span of raised floor tiles covered by the hp server footprint.

Typical Raised Floor Site

This section contains an example of a computer room raised floor system that is satisfactory for the installation of an hp server.

Based on specific information provided by Hewlett-Packard, Tate Access Floors has approved its Series 800 all-steel access floor with bolt-together stringers and 24 in. (61.0 cm) by 24 in. (61.0 cm) floor panels.

In the event that the flooring is being replaced or a new floor is being installed, Tate Access Floors recommends its Series 1250 all-steel access floor with bolt-together stringers and 24 in. (61.0 cm) by 24 in. (61.0 cm) floor panels be used to support the hp installation.

NOTE If the specific floor being evaluated or considered is other than a Tate Series 800 floor, the specific floor manufacturer must be contacted to evaluate the floor being used.

The following table lists specifications for the Tate Access Floors Series 800 raised floor system.

Table C-3 Typical Raised Floor Specifications

Item[a]	Rating
Dead load	7 lb/ft 2 (34.2 kg/m2)
Live load	313 lb/ft 2 (1528.3 kg/m2)
Concentrated load[b]	1250 lb (567 kg)

2.959 fls

Table C-3 Typical Raised Floor Specifications (Continued)

Item[a]	Rating
Ultimate load	4000 lb (1814 kg) per panel
Rolling load	400 lb (181 kg)
Average floor load	500 lb (227 kg)

a. From Table C-2 on page 203
b. With 0.08 in (0.2 cm) of span maximum deflection

Windows

Avoid housing computers in a room with windows. Sunlight entering a computer room may cause problems. Magnetic tape storage media is damaged if exposed to direct sunlight. Also, the heat generated by sunlight places an additional load on the cooling system.

RQS Nº 05/2005 - CN
CPMI - CORREIOS
0115
Fls: 3701
Doc:

Space Requirements

This section contains information about space requirements for an hp server. This data should be used as the basic guideline for space plan developments. Other factors, such as airflow, lighting, and equipment space requirements must also be considered.

Delivery Space Requirements

There should be enough clearance to move equipment safely from the receiving area to the computer room. Permanent obstructions, such as pillars or narrow doorways, can cause equipment damage.

Delivery plans should include the possible removal of walls or doors.

Operational Space Requirements

Other factors must be considered along with the basic equipment dimensions. Reduced airflow around equipment causes overheating, which can lead to equipment failure. Therefore, the location and orientation of air conditioning ducts, as well as airflow direction, are important. Obstructions to equipment intake or exhaust airflow must be eliminated.

The locations of lighting fixtures and utility outlets affect servicing operations. Plan equipment layout to take advantage of lighting and utility outlets. Do not forget to include clearance for opening and closing equipment doors.

Clearance around the cabinets must be provided for proper cooling airflow through the equipment.

If other equipment is located so that it exhausts heated air near the cooling air intakes of the hp server cabinets, larger space requirements are needed to keep ambient air intake to the hp server cabinets within the specified temperature and humidity ranges.

Space planning should also include the possible addition of equipment or other changes in space requirements. Equipment layout plans should also include provisions for the following:

- Channels or fixtures used for routing data cables and power cables
- Access to air conditioning ducts, filters, lighting, and electrical power hardware
- Power conditioning equipment
- Cabinets for cleaning materials
- Maintenance area and spare parts

Floor Plan Grid

A floor plan grid is used to plan the location of equipment in the computer room. In addition to its use for planning, the floor plan grid should also be used when planning the locations of the following items:

- Air conditioning vents
- Lighting fixtures
- Utility outlets
- Doors
- Access areas for power wiring, air conditioning filters and equipment cable routing.

2.957
fls

Typical Installation Schedule

The following schedule lists the sequence of events for a typical system installation:

- 60 days before installation
  - — Floor plan design completed and mailed to Hewlett-Packard (if required to be an HP task)
- 30 days before installation
  - — Primary power and air conditioning installation completed
  - — Telephone and data cables installed
  - — Fire protection equipment installed
  - — Major facility changes completed
  - — Special delivery requirements defined
  - — Site inspection survey completed
  - — Delivery survey completed
  - — A signed copy of the site inspection and delivery survey mailed to Hewlett-Packard
  - — Site inspection and predelivery coordination meeting arranged with a Hewlett-Packard representative to review the inspection checklist and arrange an installation schedule.
- 7 days before installation
  - — Final check made with an Hewlett-Packard site preparation specialist to resolve any last minute problems

NOTE Not all installations follow a schedule like the one noted above. Sometimes, an hp server is purchased through another vendor which can preclude a rigid schedule. Other conditions could also prevent following this schedule. For those situations, consider a milestone schedule.

- Site Preparation - schedule with the customer as soon as possible after the order is placed.
- Site Verification - schedule with the customer a minimum of one to two days before the hp server is scheduled to be installed.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0116
Fls:
Doc: 3701

ECT 2.956 June

Site Inspection

Table C-4 Customer and Hewlett-Packard Information

Customer Information	
Name:	Phone No:
Street Address:	City or Town:
State or Province:	Country
Zip or postal code:	
Primary customer contact:	Phone No.:
Secondary customer contact:	Phone No.:
Traffic coordinator:	Phone No.:
Hewlett-Packard information	
Sales representative	Order No:
Representative making survey	Date:
Scheduled delivery date	

2.955 June

Table C-5 Site Inspection Checklist

Please check either Yes or No. If No, include comment# or date				Comment or Date
Computer room				
No.	Area or condition	Yes	No	
1.	Is there a completed floor plan?			
2.	Is there adequate space for maintenance needs? Front 36 in (91.4 cm) minimum, Rear 36 in (91.4 cm) minimum are recommended clearances.			
3.	Is access to the site or computer room restricted?			
4.	Is the computer room structurally complete? Expected date of completion?			
5.	Is a raised floor installed and in good condition?			
6.	Is the raised floor adequate for equipment loading?			
7.	Are there channels or cutouts for cable routing?			
8.	Is there a remote console telephone line available with an RJ11 jack?			
9.	Is a telephone line available?			
10.	Are customer supplied peripheral cables and LAN cables available and of the proper type?			
11.	Are floor tiles in good condition and properly braced?			
12.	Is floor tile underside shiny or painted? If painted, judge the need for particulate test.			
Power and lighting				
No.	Area or condition	Yes	No	
13.	Are lighting levels adequate for maintenance?			
14.	Are there AC outlets available for servicing needs? (i.e. vacuuming)			
15.	Does the input voltage correspond to equipment specifications?			
15A	Is dual source power used? If so, identify type(s) and evaluate grounding.			

RDS Nº 93/2005 - CN
CPMI - CORREIOS
0117
Fls:
Doc: 37 01

Table C-5 Site Inspection Checklist (Continued)

Please check either Yes or No. If No, include comment# or date				Comment or Date
16	Does the input frequency correspond to equipment specifications?			
17.	Are lightning arrestors installed inside the building?			
18.	Is power conditioning equipment installed?			
19.	Is there a dedicated branch circuit for equipment?			
20.	Is the dedicated branch circuit less than 250 feet (72.5 meters)?			
21.	Are the input circuit breakers adequate for equipment loads?			
Safety				
No.	Area or condition	Yes	No	
22.	Is there an emergency power shut-off switch?			
23.	Is there a telephone available for emergency purposes?			
24.	Is there a fire protection system in the computer room?			
25.	Is antistatic flooring installed?			
26.	Are there any equipment servicing hazards (loose ground wires, poor lighting, etc.)?			
Cooling				
No.	Area or condition	Yes	No	
27.	Can cooling be maintained between 20 °C and 55 °C (up to 5000 ft.)? Derate 1 °C/1000 ft. above 5000 ft. and up to 10,000 ft.			
28.	Can temperature changes be held to 10 °C per hour with tape media? Can temperature changes be held to 20 °C per hour without tape media?			
29.	Can humidity level be maintained at 40% to 60% at 35 °C noncondensing?			
30.	Are air conditioning filters installed and clean?			
Storage				

2.953
Fls.

Table C-5 Site Inspection Checklist (Continued)

Please check either Yes or No. If No, include comment# or date				Comment or Date
No.	Area or condition	Yes	No	
31.	Are cabinets available for tape and disc media?			
32.	Is shelving available for documentation?			
Training				
No.	Area or Condition			
33	Are personnel enrolled in the System Administrator's Course?			
34	Is on-site training required?			

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 0118
Doc 3701

ECT 2.952 June

Delivery Survey

The delivery survey forms list delivery or installation requirements. If any of the items on the list apply, enter the appropriate information in the areas provided on the form.

Special instructions or recommendations should be entered on the special instructions or recommendations form. The following list gives examples of special instructions or issues:

- Packaging restrictions at the facility, such as size and weight limitations
- Special delivery procedures
- Special equipment required for installation, such as tracking or hoists
- What time the facility is available for installation (after the equipment is unloaded)
- Special security requirements applicable to the facility, such as security clearance

2.951
June

Figure C-2 Delivery Survey (Part 1)

DELIVERY CHECKLIST

DOCK DELIVERY

Is dock large enough for a semitrailer? Yes _____ No _____

Circle the location of the dock and give street name if different than address.

North

West East

South

STREET DELIVERY

Circle the location of access door and list street name if different than address.

North

West East

South

List height _____ and width _____ of access door.

List special permits (if required) for street delivery.

Permit type: Agency obtained from:

_____ _____

_____ _____

60SP018A
12/7/99

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 0119
Doc: 3701

Figure C-3 Delivery Survey (Part 2)

ELEVATOR

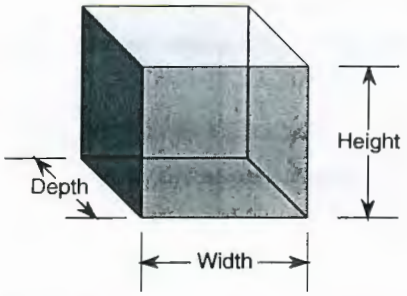
Fill in the following information if an elevator is required to move equipment.

Capacity (lb or kg) _____

Depth _____

Height _____

Width _____



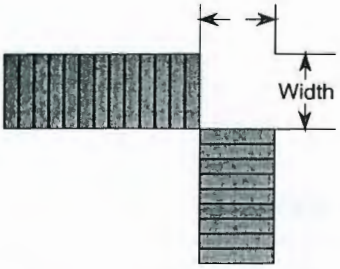
STAIRS

Please list number of flights and stairway dimensions.

Number of flights _____

Width _____

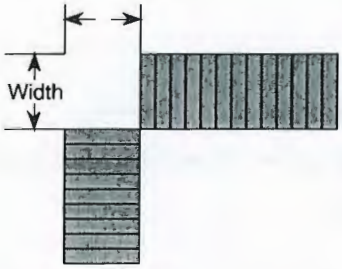
Width _____



Number of flights _____

Width _____

Width _____



60SP019A
11/24/99

2.949
Irene
CPMI - CAC

A

Accessing Error Chassis Logs, 98
Acoustic Safety Standards, 248
Adding Users, 71, 80, 83
Additional Components, 22
Altitude Operation Standards, 249
  Effects of Altitude, 249

C

Cabinet Performance Grounding (High Frequency Ground), 255
Changing the Default GSP Configuration, 82, 85
Chassis Code to FRU Decode, 93
Computer Room Physical Space Requirements, 243
  Aisle Space, 243
  Server, 243
Computer Room Unpacking Space, 244
Configure Remote Console, 60
Configure RS-232 Console, 56
Configure System Consoles, 55
Configure the LAN Console, 61
Configure the Web Console, 63
Configuring the GSP LAN Port, 80, 83
Configuring the GSP LAN Port via an ASCII console, 61
Configuring the Rev A Guardian Service Processor (GSP), 80
Configuring the Rev B Guardian Service Processor (GSP), 83
Core I/O Connections, 50
Core I/O Removal, 146
Core I/O Replacement, 147
CPU Removal, 182
CPU Socket Replacement, Cleaning, and CPU Replacement, 183
  Cleaning Kit Components, 183
  CPU Cleaning for System Board Replacement, 185, 186
  Replacing the CPU, 187
  Tools Required, 183
Cross-Referencing Chassis Log Errors to rp54xx FRUs, 93
CRU Physical Location, 216
Customer Replaceable Unit Part Numbers, 219

D

Data Communications Cables, 257
Determine Current System State, 88
Dimensions, 242
Disk Media Backplane Removal, 212
Disk Media Backplane Replacement, 213
Disk Media Housing Removal, 188
Disk Media Housing Replacement, 189
Display Board Removal, 173, 174
  Removing rp5400 and/or rp5450 Model Platform Monitors, 175
  Removing The rp5470 Model Platform Monitor, 175

E

Electrical, 245
  Modular PDUs, 246
  Office High Availability Requirements, 245
    Server-level Enhanced Power Availability, 245
  Power Protection, 245
  System Power Requirements, 246
electrical and environmental guidelines
  electrical conduit ground, 255
  electrostatic discharge prevention, 248
  lighting requirements, 252
  main building electrical ground, 255
  power panel grounds, 255
Electrical Conduit Ground, 255
electrical load requirements, 253
Environment Elements
  Acoustics, 262
Environmental Elements, 258
  Computer Room Preparation, 258
  Cooling Requirements, 258
    Air Conditioning Ducts, 260
    Air Conditioning System Guidelines, 259
    Air Conditioning System Installation, 260
    Air Conditioning System Types, 259
    Basic Air Conditioning Equipment Requirements, 258
    Basic Air Distribution Systems, 259
  Delivery Survey, 272
  Dust and Pollution Control, 260
  Electrostatic Discharge (ESD) Prevention, 262
  Facility Characteristics, 263
    Floor Loading, 263
    Average Floor Loading, 264
    Floor Loading Terms, 263
    Raised Floor Loading, 263
    Typical Raised Floor Site, 264
    Windows, 265
  Humidity Level, 260
  Metallic Particulate Contamination, 261
  Site Inspection, 268
  Space Requirements, 266
    Delivery Space Requirements, 266
    Floor Plan Grid, 266
    Operational Space Requirements, 266
  Typical Installation Schedule, 267
Equipment Grounding Implementation Details, 257
Example of Accessing Error Logs, 98
Expansion I/O LED States, 116
Extend the Server out the Front, 133

F

Factory Integrated Cabinet Installation, 2
Fan, Power Supply, and Disk LED States, 121
Field Replaceable Unit Part Numbers, 235
Front Bezel Removal (Single Piece), 142
Front Bezel Removal (Two Piece), 144
Front Bezel Replacement (Single Piece), 143
Front Bezel Replacement (Two Piece), 145
FRU Physical Location, 221

G

Graphics Troubleshooting, 46
grounding systems

RQS Nº 2002005 - CN
CPMI - CORREIOS
Fls: 0120
Doc: 3701

electrical conduit ground, 255
GSP Cables, 56
GSP Configurable Parameters, 71
GSP Features, 53
GSP LAN, 53
GSP LED States, 118
GSP RS-232, 53
Guardian Service Processor (GSP) Overview, 53

H

hot swap procedure
software, 151
HotPlug
Hardware HotPlug Procedure, 156
Hot Swap Procedure for Unattached Physical Volumes, 158
Hot Swap Software Procedure for Attached Physical Volumes, 157
HotPlug Disk Drive Removal, 151
HotPlug Disk Drive Replacement, 156
HotSwap Card Cage Fan Removal, 163
HotSwap Card Cage Fan Replacement, 164
HotSwap Chassis Fan Cover Removal, 159
HotSwap Chassis Fan Cover Replacement, 160
HotSwap Chassis Fan Removal, 161
HotSwap Chassis Fan Replacement, 162
HotSwap Power Converter Fan Removal, 167
HotSwap Power Converter Fan Replacement, 168
HotSwap Power Supply Removal, 165
HotSwap Power Supply Replacement, 166

I

Identifying Approved Non-E-Series HP Cabinets, 17
Identifying E-Series HP Cabinets, 18
Identifying Static Rail Kit, 18
Individual Component Remove/Replace Instructions, 133
Initial Power-up, 76
Insert the Server from the Front, 134
Install Deskside server, 8
Install Stand-Alone Server in a Cabinet, 11
Installing a PCI Card, 36
Installing Central Processing Units (CPUs), 23
Installing Disk Drives, 47
Installing Graphics, 39
Installing Memory, 28
Installing Peripheral Component Interconnect (PCI) Cards, 32
Installing rp5400 and/or rp5450 DIMMs, 28
Installing rp5470 DIMMs, 30
Installing Stationary Rails, 19
Interpreting Chassis Logs Using the chassis_code.codes File, 100
Interpreting Service Processor Error Chassis Logs, 98
Interpreting System Alerts, 96, 97

K

Key FRU Identification Fields for Error Chassis Logs, 99
Key FRU Identification Fields for System Alerts, 97

L

Power Distribution Safety Grounding, 255
Site Preparation
Distribution Hardware
Raceway Systems (electrical conduits), 254
LAN and Telephone, 247
LAN/SCSI LED States, 120
lighting requirements, 253

M

Memory Configuration Rules, 28
Memory DIMM Removal, 171

Removing rp5400 Memory DIMMs, 171
Removing rp5470 Memory DIMMs, 171
Memory DIMM Replacement, 172
Replacing rp5400 and/or rp5450 Memory DIMMs, 172
Replacing rp5470 Memory DIMMs, 172

O

Online Addition/Replacement (OLA/R) of PCI I/O cards, 38

P

PCI Backplane Removal, 206
Removing rp5400 and/or rp5450 PCI Backplanes, 206
Removing rp5470 PCI Backplane, 207
PCI Backplane Replacement, 209
Replacing rp5400 and/or rp5450 PCI Backplanes, 209
Replacing rp5470 PCI Backplane, 211
PCI Card Separator/Extractor Removal, 149
PCI Card Separator/Extractor Replacement, 150
PCI I/O Card Installation Order, 34
PCI I/O Card Installation Restrictions, 34
PCI I/O Card Removal, 179
PCI I/O Card Replacement, 180
PCI I/O LED States, 114
Platform Monitor Replacement, 177
Replacing rp5400 and/or rp5450 Platform Monitors, 177
Replacing rp5470 Platform Monitor, 177
Power Converter Removal, 193
Power Converter Replacement, 194
Power Panel Ground, 255
Power Supply Failure Example, 95
Problem Symptoms and Repair Actions, 89
Processor Failure Example, 95
Processor Support Module Removal, 169
Processor Support Module Replacement, 170

R

raised floor
ground system, illustrated, 256
Raised Floor "High Frequency Noise" Grounding, 256
Receive/Unpack A Non-Integrated Server, 5
Removable Media Removal, 190
Removable Media Replacement, 191

SCSI ID Settings, 191
Remove and Replace Procedures by Part, 124
Removing Users, 72, 82, 85
Return the GSP to Default Configurations, 73
Revision A GSP, 50, 54
Revision B GSP, 51, 54
rp5400 and rp5450 I/O Block Diagram, 103
rp5400 and rp5450 System Block Diagram, 102
rp5400/rp5450 PCI Card Slots, 32
rp5430 and rp5470 System Block Diagram, 104, 105
rp5470 PCI Card Slots, 33
rp54xx Server Boot Process, 74
Run/Attention/Fault LED States, 106

S

Sample System Alerts, 97
Secure Web Console Installation, 68
Side Cover Removal, 140
Side Cover Replacement, 141
Site Preparation
  Computer Room Safety, 252
    Fire Protection, 252
    Lighting Requirements for Equipment Servicing, 252
  Distribution Hardware, 254
    Building Distribution, 254
    Wire Selection, 254
  Electrical Factors, 252
  Electrical Load Requirements (Circuit Breaker Sizing), 253
  Grounding Systems, 255
  Power Consumption, 253
  Power Quality, 253
    Power System Protection, 254
    Sources of Voltage Fluctuations, 253
Space Requirements, 242
Stand-alone Server Cover Removal, 135
Stand-alone Server Cover Replacement, 137
Stationary L-Bracket Rail Assembly, 17
System Board Removal, 195
  Removing rp5400 and/or rp5450 Model System Boards, 195
  Removing rp5470 Model System Board, 196
System Board Replacement, 197
  rp5400 or rp5450 System Board Replacement, 197
    Configuring System Board, 198
  rp5470 System Board Replacement, 201
    Power up procedure., 204
System Installation Guidelines, 257

T

Temperature and Humidity Operating Standards, 250
  Thermal Protection Features, 250
Top Cover Removal, 138
Top Cover Replacement, 139
Troubleshooting and FRU identification, 89

U

Uncrating Space, 242
Unpacking the SPU, 5

V

V-Class system
  temperature and humidity specifications, 250

W

Wiring Connections, 257

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0121
Fls:
3701
Doc:

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0122
Fls:
3701
Doc:

2.944
brasil

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

hp servers rp5430 and rp5470

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.

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

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0123
Fls:
Doc: 3701
3701

proven solutions for business-critical computing

2.945 Bruno

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.

ROS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 0124
Doc: 3701

2.944
Irene

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, o 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 dato
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 [illegible] de-allocation, dynamic processor resilience, and de-allocation of [illegible]cation 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 avoidonce, 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, ot an affordable price
3-yeor 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

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0125
Fls:
Doc: 3781

F C T
2.943
fls

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 quod-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

ctromagnetic 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

ontact 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.

© Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice. 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.

Intel and Itanium are registered trademarks of Intel Corporation in the United States and 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. Windows is a U.S. registered trademark of Microsoft Corporation.

06/12/03
5980-8432EN Rev. 6

invent

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 0126
3701
Doc:

Apêndice AD

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 0127
Doc: 3701

2.942

invent

hp services | SAN environment support | data sheet

storage area network environment support

overview

To meet the needs of IT managers and storage area network (SAN) administrators in maintaining critical SAN environments, HP offers HP SAN Environment Support. Designed to maximize SAN uptime and stability, and minimize interoperability issues, HP SAN Environment Support provides you with a single source for reactive and proactive support for your HP SAN environment and multivendor SAN infrastructure.

With HP SAN Environment Support, you are assigned a SAN-peaked account support engineer (ASE) who proactively works with you to maximize SAN availability and stability. The standard duties of your SAN ASE include regular SAN availability reviews, SAN topology mapping and maintenance, firmware upgrade planning and implementation, plus change management planning and assistance. In addition to these standard activities, your ASE can help you in other ways, including assistance in ongoing use of SAN management software, SAN upgrade planning, direct-connect-to-SAN conversion assistance, and SAN-based back-up planning.

HP SAN Environment Support also provides a single point of contact for reactive HP SAN environment and multivendor SAN infrastructure support. This feature, delivered by HP SAN support experts, eliminates the need for your IT staff to make multiple calls to multiple vendors to resolve interoperability problems. Efficient problem resolution and elimination of finger pointing is facilitated by HP's alliance with Brocade Communications Systems, Inc. Additionally, to accelerate the troubleshooting process, HP has also developed a suite of SAN diagnostic tools.

HP SAN Environment Support provides you with global resources and expertise to supplement your own internal IT staff, enabling them to focus on core business issues.

benefits to you

- Increase business productivity through increased SAN availability.
- Prevent problems from occurring, through regular reviews with an HP SAN expert.
- Reduce the risks and improve the effectiveness of changes by proactively managing changes in your SAN environment.
- Improve SAN stability with firmware upgrade planning and implementation from an HP SAN expert.
- Call on a single source for quick and accurate reactive resolution of complex multi-vendor SAN interoperability problems, with minimum disruption to your users and IT managers.
- Increase the effectiveness of IT staff, so they have more time to focus on core business issues.
- Alleviate the difficulty of recruiting, training, and retaining SAN experts.

PREMIER Qualified Support Partner

Premier Brocade Qualified Support Partner

IRQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 0128
Doc: 5701

table 1. service feature highlights

support team	proactive features	reactive features
• Assigned SAN-peaked ASE • HP Response Center SAN support experts	Prevention of problems and proactively managing changes are preferable to even the fastest crisis response. HP SAN Environment Support offers a comprehensive suite of standard and selectable proactive account services delivered by a SAN-peaked ASE. Standard services include: • Initial SAN assessment • SAN support plan • Maintenance of SAN documentation • Firmware upgrade planning and implementation • Change management planning and assistance • Ongoing participotion in management and administration of the SAN • Mid-year SAN review • Year-end briefing selectable services include: • Assistance in ongoing use of SAN management software • SAN upgrade planning assistance • Direct-connect-to-SAN conversion assistance • SAN-based back-up planning • Additional change management planning and assistance	HP provides you with a single source for HP SAN environment and multivendor SAN infrastructure support, including: • Phone-in assistance from a SAN support expert • SAN troubleshoating and fault isolation • One-stop problem management • SAN fabric OS support • HP SAN diagnostic tools • Support alliance with Brocade Communications Systems, Inc. • Escalation management • Flexible call submittal coverage • Optional 24x365 call submittal

support program specifications

table 2. support team

feature	delivery specification
ASE	Your ASE is your SAN support manager and technical expert. Your ASE serves as a trusted advisor. Working closely with your technical staff and IT management, your ASE provides guidance to help maintain your SAN environment by identifying and delivering the services that best suit your business needs. To help meet your business objectives, your ASE works with you to develop and routinely review a mutually agreed upon SAN support plan. As standard services, your ASE also maintains your SAN topology map, conducts SAN reviews, assists with firmware upgrade planning and implementation for SAN components, provides change management planning and assistance, transfers knowledge of best practices, and also participates in your internal meetings when required.
HP Response Center SAN experts	Our team of industry-leading SAN support experts is available to provide troubleshoating, fault isolation, and problem resolution for multivendor SAN infrastructures.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0129
Fls:
Doc: 3701

table 3. proactive features

feature or service	specifications
standard services	The foundation of HP SAN Environment Support is a suite of services that HP provides to address your high availability SAN needs.
Initial SAN assessment	During the initial assessment, your ASE fully documents your SAN, including SAN topology: firmware levels of hosts, fibre channel switches, and other fibre channel devices; patch levels of hosts; and versions of SAN management software. Based on this information, your ASE assesses the supportability of your SAN. Your ASE identifies any weaknesses within your SAN that could affect availability or supportability and makes recommendations for change. The recommendations and SAN documentation are provided to you in the SAN support plan. If your SAN has recently been implemented using HP's SAN Implementation Service, this activity may not be required. If this is the case, your ASE will advise you regarding additional activities that can be performed in lieu of this service.
SAN support plan	The SAN support plan documents your SAN topology and configurations and the logistics of how support will be delivered to you, and sets clear expectations for the support relationship. Your ASE meets with you to develop your SAN support plan. In the case of an HP mission critical computing or storage environment, your ASE can integrate the SAN support plan into your existing account support plan.
Ongoing maintenance of SAN documentation	Your ASE works with you to maintain an up-to-date snapshot of your SAN. This vital activity supports fault isolation, daily operation, and planning for future growth.
ware upgrade planning and implementation	Your ASE works with you to develop an implementation plan for firmware upgrades on your SAN switches. He or she will identify considerations, pitfalls and recommendations related to your unique SAN environment. For HP and non-HP fibre channel switches covered by an HP support contract, an HP customer engineer (CE) installs the firmware upgrades as agreed to in the implementation plan.
Change management planning and assistance	Your ASE helps minimize risks and possible disruptions when implementing changes to your SAN. Utilizing industry best practices, your ASE helps you avoid the pitfalls that are often associated with changes to your SAN environment.
Ongoing participation in management and administration of the SAN	Your assigned ASE participates and assists in SAN activities, both technical and operational, as you require. Your ASE serves as a trusted advisor for issues that may arise with your SAN.
Mid-year review	Your ASE conducts a mid-year review. Your ASE reviews the status of your SAN for stability, performance, and supportability, including any open issues. The ASE makes any recommendations necessary to ensure that problems do not recur. The work done to date by HP is also reviewed. Your plans for SAN upgrades are addressed, as well as your needs for any additional selectable SAN services.
Annual review	HP provides you with an annual review, based on a report that summarizes the availability of your SAN during the support year and itemizes the technical services and account management activities you received.
Selectable services and activities	In addition to providing standard services, HP SAN Environment Support also offers a range of additional SAN services. These services are designed to improve the ongoing management and availability of your SAN. The duration of each service will vary with the complexity of your SAN and your individual needs. Your ASE can advise on the service deliverables and duration. You are entitled to at least one selectable service. Your ASE may be able to provide more selectable services, depending on the amount of time each service requires. The selectable services include: • Assistance in ongoing use of SAN management software • SAN upgrade planning assistance • Direct-connect-to-SAN conversion assistance • SAN-based back-up planning • Additional change management planning and assistance

IRQS Nº 03/2005 - CN
CPMI - CORREIOS
0130
Fls:
Doc: 3701

table 4. reactive support

feature	delivery specifications
Phone-in assistance from a SAN support expert	This feature provides unlimited, toll-free (where available) phone access for authorized callers to the HP Response Center. When your call is received at HP, on HP SAN support engineer quickly responds to gather information about the problem and begins work. With your authorization, the engineer remotely accesses your SAN to run diagnostics. Assistance is available Monday through Friday, excluding HP holidays, during standard HP Response Center hours. Optional coverage is also available 24 hours per day, 365 days per year.
SAN troubleshooting and fault isolation	HP will troubleshoot and fault isolate your HP SAN environment and multivendor SAN infrastructure. (SAN infrastructure is defined to include switches, hubs, bridges, and fibre channel host bus adapters [hbas]). If you have nan-HP hosts or storage devices within your SAN not covered by HP maintenance contracts, troubleshooting and fault isalatian an these products is limited to the identification of interoperability issues related to the host operating system or storage device firmware versions. SANs are camprised of complex combinations of switches, storage devices, hbas, hast operating systems and the variaus settings, device drivers, and firmware acrass these components. Drowing fram its extensive knowledge and experience in these complex environments, HP can effectively troubleshoot problems and moke recommendations regarding which settings or versians yield favorable results. HP SAN support engineers provide netwark troubleshooting and identification of the specific saurce of connectivity problems within the specified SAN infrastructure. Sources of SAN faults are isalated to specific hardware products and network cabling. Traubleshooting covers the following issues: • Identification of connectivity problems related to incorrectly configured fibre channel switches. • Identificatian of cannectivity problems caused by interoperability issues between the fibre channel switch, hba or storage device firmware, host operating systems revisions, or hba drivers. • Identificatian af physical connectivity prablems between two network devices, such as physical infrastructure problems related to cables and hbas. • Identification of problems related to faulty SAN devices, network bandwidth excess utilization, or existing faulty SAN design. For simple design-related performance problems, your ASE can assist as part of the ongoing participation in the management and administration of your SAN.
One-stop problem management	HP acts as a single point of contact to manage problems identified through the fault isolation process. Focusing on your complete HP SAN environment and multivendar SAN infrastructure, HP will take the following actions: • HP will advise on changes needed to remedy interoperability problems between switch, hba or storage device firmware, or host operating system and hba drivers. For HP and non-HP products that are covered under HP's software and hardware maintenance support agreements, HP will implement the necessary changes needed to resolve an interoperability problem. • For SAN infrastructure devices not covered by HP support agreements, HP can act as an agent to deal, on your behalf, with your non-HP SAN product vendars. As your appointed agent under an Agency Agreement, HP will contact the vendor to initiate the necessary action and fallow up with the vendor until the problem is resolved. • For SAN infrastructure products not covered by HP hardware or software support agreements or an Agency Agreement with HP, the HP SAN support engineer will provide you with detailed information on the identified problem device(s) to help you work with your vendor. • If a change is recommended to the firmware version on a storage device or the operating system on a host not covered by HP support agreements, HP will provide you with detailed information to help you work with your vendor.
SAN fabric operating system support	As part of the HP SAN Environment Support troubleshooting process, HP may recommend which version of SAN fabric operating system will yield the most favorable operating results. For fibre channel switches covered by an HP support contract, HP will be able to supply the necessary firmware operating system upgrade. As part of the initial SAN assessment and change management service, HP will also advise you on which versions of host operating systems, device drivers, and storage device firmware will work best with your version of SAN fabric operating system.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0131
Fls:
Doc: 370

HP SAN diagnostic tools	HP's SAN diagnostic tools speed up the troubleshooting process ond improve resolution time by: • Collecting host, hba, operating system, switch, and array configuration information. • Providing a Web-based SAN topology navigator, which enables the support engineer to hierarchically create the complete support environment, including diagramming the physical connection between SAN devices. • Diagramming the physical connection between SAN devices.
Support alliances with Brocade Communications Systems, Inc.	Through the coordinated efforts of HP and Brocade Communications Systems, Inc., support experts, you receive timely, efficient and effective problem resolution. HP is a Premiere Qualified Support Partner for Brocade Communications Systems, Inc. Our SAN experts benefit from each company's extensive SAN interoperability test data, expertise, and resources. HP's service and support alliance with Brocade provides you with the following: • HP engineers with the highest level of training and technical backup support available for Brocade products and SAN fabric OS. • Investments in support laboratory facilities to simulate SAN problems for Brocade SAN devices. • Access to Brocade engineering teams for fast-track backup support and problem resolution, as well as access to Brocade's support databases.
Escalation management	HP has established formal escalation procedures to solve complex SAN problems. Local HP management coordinates problem escalation, rapidly enlisting the skills of key problem-solving experts throughout HP, as well as third-party product vendors for which HP is an Authorized Service Provider. At HP's discretion, the HP Response Center may dispotch an HP engineer to your site to assist with problem resolution. In most cases, resources arrive within one working day, if your site is within 100 miles (160 km) of the nearest primary HP Support Responsible Office.
Flexible electronic call submittal	Authorized callers can submit calls electronically to the HP Response Center, via the HP Electronic Support Center, and request a call back within two hours (or the next business day if after standard hours) or a written electronic response by the next business day.

table 5. related services

feature	delivery specifications
24x365 coverage option	This option provides additional coverage hours for remote assistance for SAN problems. Unlimited, toll-free access to the HP Response Center is available to authorized callers. Assistance is available 24 hours per day, 365 days per year, including weekends and holidays, for all eligible HP products and selected non-HP SAN devices.

additional program features

your responsibilities

As part of HP SAN Environment Support, you must assign a Customer SAN Support Manager. This person works in partnership with the assigned HP ASE to coordinate support activities, prioritize utilization of HP SAN Environment Support, and monitor corresponding responsibilities. In order to speed up the troubleshooting process it is strongly recommended that you provide dial-up access into the SAN to HP engineers.

In order to minimize the risks associated with making changes to the SAN, you must communicate to the HP support team all pending hardware, software, or network changes.

You must designate two people to serve as your authorized callers to HP's Response Centers regarding SAN issues.

coverage boundaries

Your SAN must be operational before SAN Environment Support commences.

For storage devices and hosts within your SAN environment that are not covered by an HP hardware or software support contract, fault isolation and troubleshooting is limited to the identification of interoperability issues related to the host operating system or storage device firmware versions.

For SAN components not covered by an HP hardware or software support agreement, one-stop problem management is only offered on the SAN infrastructure, defined to include switches, hubs, bridges, and fibre channel hbas.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 0132
Doc: 3701

This service:

- Is not available for SANs containing non-HP director class fibre channel switches.
- Is offered only for fibre channel-based SANs; it currently does not cover iSCSI SANs
- Is not available for SANs that use switches with copper GBICS
- Is applicable to SANs with up to 256 switch ports and three (3) operating systems.
- Coverage for more complex SANs can be arranged with a custom quotation.

To verify the supportability of your SAN, your ASE will use both HP and Brocade interoperability tests and certification results and configuration matrices. If you wish to employ a component not tested or certified by HP or Brocade, HP may support this component on a "best effort" basis. This will apply only if the given unit was functioning normally when HP mapped the environment and commenced SAN Environment Support. In this case, HP's response will be limited to the following activities, if a previously functioning unit exhibits a condition interfering with the normal operation of the SAN and the customer's business operation:

- Assist and coordinate activities with applicable third party vendors
- Verify fabric connectivity using device-independent commands and feature sets resident in the switches or fabric
- Verify host connectivity using standard OS commands on supported operating systems

While these activities may resolve the problem, HP will not retain accountability for restoring unsupported devices, appliances, or adapters to normal function, nor is HP accountable to resolve issues with unsupported items resulting from a SAN or infrastructure upgrade.

coverage hours

HP SAN Environment Support provides coverage during standard business hours. See Table 5 for more information on 24x365 support availability.

Proactive services are performed during standard business hours.

ordering information

HP SAN Environment Support provides coverage for your SAN environment—not just the devices. The price of the service is determined by the size and complexity of your storage network environment.

HP SAN Environment Support is available for SANs with up to 256 switch ports and three (3) operating systems. Coverage for more complex SANs can be arranged with a custom quotation.

HP SAN Environment Support is usually purchased for a 12-month period, billable in advance, on an annual, quarterly, or monthly basis.

When HP SAN Environment Support is purchased in conjunction with HP hardware and software support services, the coverage hours for HP SAN Environment Support must be equal to or greater than the hardware and software support coverage hours.

Some service features are subject to local availability. Service features may vary according to local resources. To obtain more information or to order HP SAN Environment Support, contact your local HP sales representative.

for more information

For more information on HP Services, contact any of our worldwide sales offices or visit our Web site at: www.hp.com/go/services.

Technical information contained in this document is subject to change without notice.

© Copyright Hewlett-Packard Company 2002. All Rights Reserved. Reproduction, adaptation, or translation without prior written permission is prohibited, except as allowed under the copyright lows.

06/2002

5980-8367EN

invent

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 0133
Doc: 3701

Apêndice AE

ROS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 0134
Doc: 3701

ECT
2.934
Irene

Format conventions

Convention	Denotes
Caution	A condition or situation that could damage Storage Area Manager, the storage network, or data stored on the network
Note	Important or clarifying information, including exceptions, interdependencies, and special situations
Tip	An action that will streamline the current procedure
bold font	Text to be entered exactly as shown; for example, commands, path names, filenames, and directory names
	Buttons and tabs to click; for example, the **Save** button
	Menu and command names
	Keys on the keyboard
`courier font`	Text displayed on the screen

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0135
Fls: 3
3701
Doc:

ECT 2.933 fune

CONTENTS

1 Storage Area Manager 1

hp OpenView storage area manager features 2
Managing hp OpenView storage area manager users 4
Adding a user 4
Managing device discovery 6
Starting device discovery 6
Stopping device discovery 7
Setting the device discovery interval 7
Managing and using device maps 9
Setting the device map mode 9
Using the layout manager 11
Configuring device links 13
Managing events 17
Acknowledging events 18
Exporting events 19
Deleting events 20
Adding event filters 23
Adding event triggers 25
Managing folders 29
Managing organizations 31
Defining an organization's properties 32
Adding members to the organization 33
Implementing in cluster environments 34
Implementing in MSCluster environments 34
How hp OpenView storage area manager operates in AIX cluster environments 36

ROS Nº 03/2005 - CN
CPMI - CORREIOS
0136
Fls: 5
Doc 3701

2 Storage Accountant 39

hp OpenView storage accountant features 40
Billing basics 42
How charges are calculated 42
How charges become bills 42
Getting started with billing 43
Service level setup and administration 45
Creating service levels 45
Setting LUN service levels 45
Deleting service levels 47
Account setup and administration 48
Adding accounts to organizations 48
Adding LUNs to accounts 49
Removing LUNs from accounts 50
Closing accounts 51
Billing configuration 52
Setting the billing period 52
Setting export options 53
Setting a billing event trigger 54
Billing data archiving 55
Setting the bill retention period 55
Setting the audit retention period 56
Archiving and restoring bills 56
Setting currency preferences 58
Integrating bills with other applications 59

ECT
2.931
fls.

3 Storage Builder 61

hp OpenView storage builder features 62
Physical and logical space 64
Definition of terms 65
About NAS devices 65
Capacity data collection 66
Scheduling capacity collection 67
Collecting interim capacity data 68
Capacity data archiving 70
Scheduling capacity summaries 70
Managed directories 72
Adding managed directories 74
Removing managed directories 75
Capacity thresholds 76
Setting domain thresholds 77
Setting organization thresholds 77
Setting thresholds on specific resources 78
Entering threshold properties 79
Deleting capacity thresholds 81
Capacity reports 82
Setting the file format of detailed file/directory lists 83
Defining file reports 83

4 Storage Node Manager 87

hp OpenView storage node manager features 88
Configuring device-specific application links 89
Adding an application link to a device 89
Adding an application link to a device model 92

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0137
Fls: 7
Doc: 3701

2.930 June

Starting device-specific application links 94
Viewing device status summary 95

5 Storage Optimizer 97

hp OpenView storage optimizer features 98
Performance metrics 100
All metrics 100
Common metrics 101
Performance data collection 103
Collection schedule 103
Enabling/disabling metrics collection 103
Performance data archiving 105
Archive retention 105
Scheduling performance archives 105
Performance baselines and automatic thresholds 107
Baseline parameters 107
Baseline limitation 108
Enabling/disabling baseline thresholds 108
Performance charts 110
Managing performance charts 112
Deleting performance charts 112
Restoring default charts 113

6 Storage Allocater 115

hp OpenView storage allocater features 116
Groups 117
Security groups 117
Organizational groups 119

ECT
2.929
fls.

Managing assignments 120
Assignment types 120
Assignment rules 121
Special unassignments 122
Assigning LUNs for Windows Clustering 125
Assigning LUNs for volume management software 128
Assigning LUNs for HP-UX and Solaris VERITAS Volume Manager Storage Administrator 129
Assigning LUNs for Windows NT stripe and volume sets 130
Managing LUNs with Windows 2000 dynamic volumes 132
Viewing assigned LUNs on HP-UX hosts 136
Managing hosts 138
Modifying Windows NT host settings 138
Moving a host from one management server to another 140
Managing a "dead" host 141
Managing LUNs 142
Viewing or modifying logical unit information 142
Viewing or deleting missing LUNs 144
hp OpenView storage allocater interoperability 145
With FC60 storage arrays 145
With AIX cfgmgr 150
With HP-UX ioscan 151
With HP-UX Storage Data Protector and hp StorageWorks virtual arrays . . . 152
With Linux device files 152
With Linux tape LUNs 158
With Linux 16-byte CDBs 158
With Linux Command View SDM 158
With Solaris HBAs 159
With Solaris tape and nondisk devices 160
With Solaris Omniback II, Data Protector, and tape libraries 163

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0138
Fls:
Doc: 3701

2.928 Irene

With Solaris SecurePath 164
With Windows NT Disk Administrator 165
With Windows NT Performance Monitor 166
With Windows NT SCSIPORT 167

7 Configuring the bridge 169

hp OpenView storage area manager bridge 170
User accounts 171
Creating Bridge user accounts 171
Multiple management servers 172
Authorizing the primary server as a client 173
Modifying the Bridge configuration file 173
SSL 174
Creating a server keystore and certificate 174
Modifying the Bridge configuration file 176
Distributing server certificates 177
Changing the default port 178

8 Troubleshooting 179

hp OpenView storage accountant 180
When the management server stops 180
Events do not appear in the event panel 182
Accounting screens do not show a currency symbol for fiscal data 183
Old bills are missing in the bill and report viewers 184
An error message appears when you create a new account or service level . 185
hp OpenView storage builder 186
A managed directory has zero used space 186
Data is unavailable in the Add Directories window 187
There is no Capacity tab 188

ECT
2.927
fls.

hp OpenView storage optimizer 189
There is "no data" in a performance list or chart 189
There is no Performance tab 190
hp OpenView storage allocater: All platforms. 191
LUNs are not listed in the Available to Assign list 191
LUN Allocation and LUN Discovery do not appear in the user interface 192
LUN Allocation and LUN Discovery are disabled in the user interface 193
Assigned LUNs are not available on a host 194
A multiple writer situation is detected 196
hp OpenView storage allocater: Windows 198
A LUN cannot be unassigned from a Windows host. 198
An assigned disk is not accessible 200
Dynamic disks are offline (Windows 2000) 201
The SCSI Adapters control panel lists no LUNs (Windows NT) 202
hp OpenView storage allocater: HP-UX 203
Verifying that the daemon is running 203
An assigned LUN is not accessible to an HP-UX host 204
Error during mounting: "not a block device". 205
A LUN cannot be unassigned from an HP-UX host. 206
A Storage Data Protector snapshot backup involving an HP-UX hosts fails. . 207
A rogue host event is displayed for an HP-UX host that is running VERITAS Volume Manager 208
hp OpenView storage allocater: Solaris 209
Error during mounting: "not a block device". 209
A LUN cannot be unassigned from a Solaris host. 210
An assigned tape library or nondisk device is not available 211
Assigned LUNs are suddenly unavailable 212
A Host with an Emulex HBA reports errors in the /var/adm/messages log. . . 213
hp OpenView storage allocater: Linux 214
A LUN cannot be unassigned from a Linux host. 214

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0139
Fls:
3701
Doc:

A Linux host cannot see RUIDs 215
A Linux host cannot see LUNs 216
You cannot assign more than 40 LUNs to a Linux host 217
The boot process hangs on a Linux host 218
hp OpenView storage allocater: AIX 219
Verifying that the daemon is running 219
A LUN cannot be unassigned from an AIX host 220

Index 221

ECT
2.925
fls.

1 STORAGE AREA MANAGER

hp OpenView storage area manager features

Managing hp OpenView storage area manager users

Managing device discovery

Managing and using device maps

Managing events

Managing folders

Managing organizations

Implementing in cluster environments

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0140
Fls:
Doc: 1701

hp OpenView storage area manager features

HP OpenView Storage Area Manager provides comprehensive, centralized management across distributed, heterogeneous storage networks. The Storage Area Manager product suite includes the following applications: Storage Node Manager, Storage Accountant, Storage Allocater, Storage Builder, and Storage Optimizer.

Among other features, Storage Area Manager provides the following regardless of which application(s) you install and license.

- *Device discovery and mapping.* Storage Area Manager automatically discovers hosts, interconnect devices, bridges, and storage devices in direct attached (Fibre Channel or SCSI) and networked storage (SAN and NAS) environments. Discovered devices are placed in the Resources tree and a device map. Storage Area Manager illustrates the relationship of these devices by displaying their links within each device map.

  If the storage network is using interconnect hardware to support fabric zoning, Storage Area Manager identifies the pre-configured zones and lists them under the Storage Networks node in the Resources tree. Storage Area Manager also creates a corresponding device map of each zone.

- *Event management.* Based on its status inquiries of the storage network and its own processes, Storage Area Manager generates and displays events in the event panel. Framework and discovery-related events are displayed regardless of which applications are installed and licensed. Device status, LUN security, performance, capacity, and billing related events only appear if the applicable application is installed and licensed.

  Storage Area Manager is able to receive SNMP traps from devices that support trap forwarding. You can also configure event triggers to perform certain actions based on event criteria. For example you can configure an event trigger to send e-mail notification to your on-call administrator for all events of a specified severity level.

ECT
2.923
June

Storage Area Manager also provides several features to manage the events that appear in the event panel. You can configure filters so only events that meet the filter's criteria are displayed in the event panel. You can also export all or selected events to a .txt, .csv, or .xml file. Finally, you can configure Storage Area Manager to automatically delete events based on a maximum number or on criteria such as event age, severity level, and category.

- *Manager of Managers.* The Manager of Managers (MoM) enables you to monitor up to 50 storage domains from one console. You can configure MoM to retrieve and display status and event information from each Storage Area Manager management server in your environment. This feature allows Storage Area Manager to easily scale in large, complex storage environments.
- *User authentication and authorization.* When starting Storage Area Manager, a user must login with their unique user name and password. Storage Area Manager user accounts can be configured with different levels of privilege. User accounts with Administrator privilege are able to save changes to the Storage Area Manager database and may perform all Storage Area Manager tasks. User accounts with Guest privilege are only able to view information provided by Storage Area Manager and are not able to save changes. User account privileges apply to tasks conducted both through the user interface and command line user interface.
- *Command Line User Interface (CLUI).* Storage Area Manager provides an extensive CLUI. Nearly all tasks that can be performed in the user interface can also be performed from the CLUI.

ROS Nº 03/2005 - CN
CPMI - CORREIOS
0141
Fls:
Doc 3701

2.922

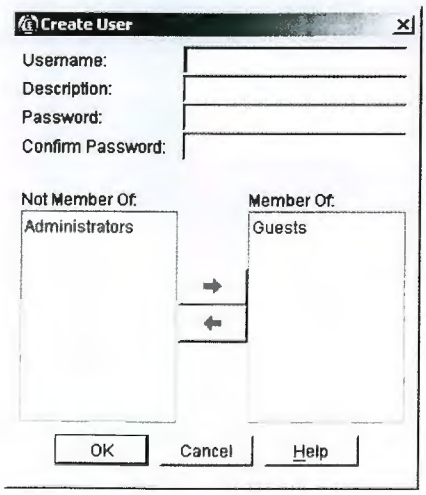
Managing hp OpenView storage area manager users

Storage Area Manager's authentication and authorization feature enables you to create users specific to Storage Area Manager. Each user is assigned to a user group, which determines the tasks that the user can perform within Storage Area Manager.

Members of the Administrators group can perform all tasks including making changes that are saved in the database. Members of the Guests group may view all information presented within Storage Area Manager, but they cannot make changes that are saved to the database.

Adding a user

1. From the **Tools** menu, select **Configure Security**. The Administer Users window appears.
2. Click the **New User** button. The Create User window appears.



3. Enter a user name for this user in the Username box.

E C T
Q. 921
Jure
C.P.I. - C.

4. Enter a description for this user in the Description box. This is an optional field and may not exceed 512 characters.
5. Enter a password for this user in the Password box.
6. Re-enter the password in the Confirm Password box. The Username and Password fields are case-sensitive.
7. Verify that the user group to which this user will be assigned appears in the Member Of box.

   To move a user group to the Member Of box, select it in the Not Member Of box, and click the right arrow button.
8. Click the **OK** button to save changes and close the window.
9. Verify that the user you created appears in the Administer Users window, and click the **Close** button to close the window.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0142
Fls: 5
Doc: 3701

Managing device discovery

Discovery is the process in which Storage Area Manager searches the storage network for devices it supports and then adds them to the database and user interface. When discovered, devices are placed under the appropriate node in the Resources tree and added to the appropriate device map.

Discovery is an ongoing process; however, you must initiate the process after installing Storage Area Manager. Completing the Setup Assistant initiates the discovery process.

Starting device discovery

Storage Area Manager provides two methods for starting device discovery. You can start a comprehensive discovery cycle in which Storage Area Manager attempts contact with each device, or you can start the ongoing discovery process in which Storage Area Manager continuously probes the storage network for changes to the device information stored in its database.

Starting a full discovery cycle

1. From the **Tools** menu, select **Start Comprehensive Discovery**. A confirmation window appears.
2. Click the **OK** button.

Starting the ongoing discovery process

1. From the **Tools** menu, select **Configure**.
2. In the Configuration window's navigation tree, select **Discovery**.
3. Select the **Yes, run discovery** radio button.
4. Click the **OK** button to save changes and close the window.

2. 919
Irene

Stopping device discovery

Device discovery is an ongoing process, however, you can instruct Storage Area Manager to stop the discovery process.

1. From the **Tools** menu, select **Configure**.
2. In the Configuration window's navigation tree, select **Discovery**.
3. Select the **No, do not run discovery** radio button.
4. Click the **OK** button to save changes and close the window.

Setting the device discovery interval

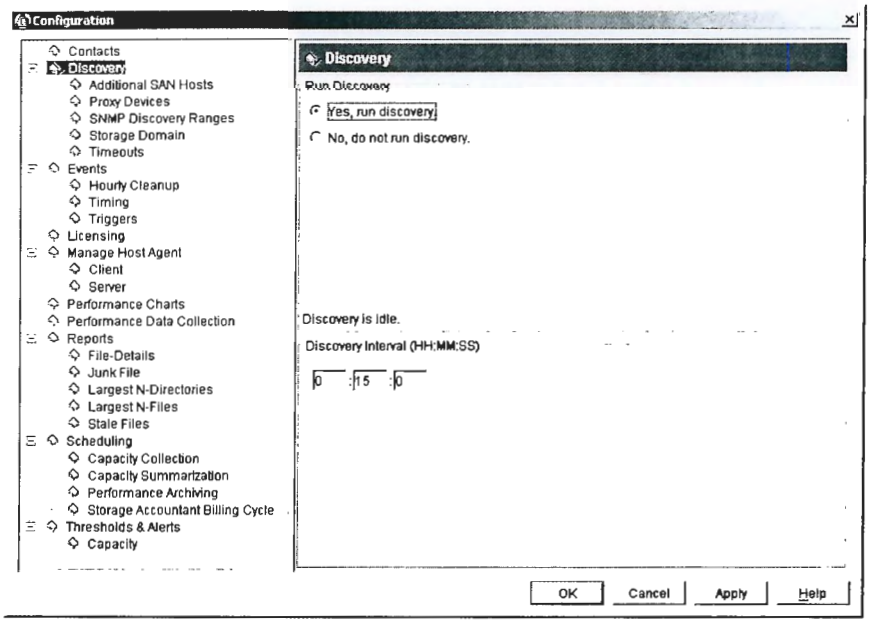
Storage Area Manager contacts each SAN host at a regular interval to obtain any new device discovery information. The default interval is 15 minutes.

Note Setting the discovery interval too low may result in higher levels of network traffic and CPU usage as well as event processing difficulty within Storage Area Manager. Hewlett-Packard recommends setting the interval no lower than the default setting of 15 minutes.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0143
Fls: 7
Doc: 3701

2.918 June

1. From the **Tools** menu, select **Configure**.
2. In the Configuration window's navigation tree, select **Discovery**.



3. Modify the hours, minutes, and seconds fields to the settings you prefer.
4. Click the **OK** button to save changes and close the window.

ECT
2.917
Brent

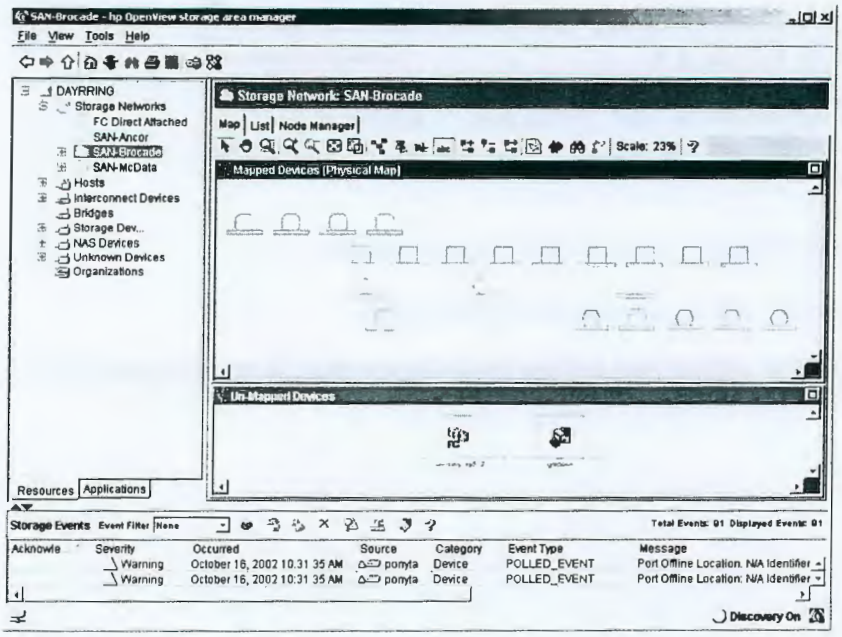
Managing and using device maps

As Storage Area Manager discovers your storage network, it places devices in device maps using default layouts. Storage Area Manager offers many features that allow you to work with the map to customize it to your preferences.

Setting the device map mode

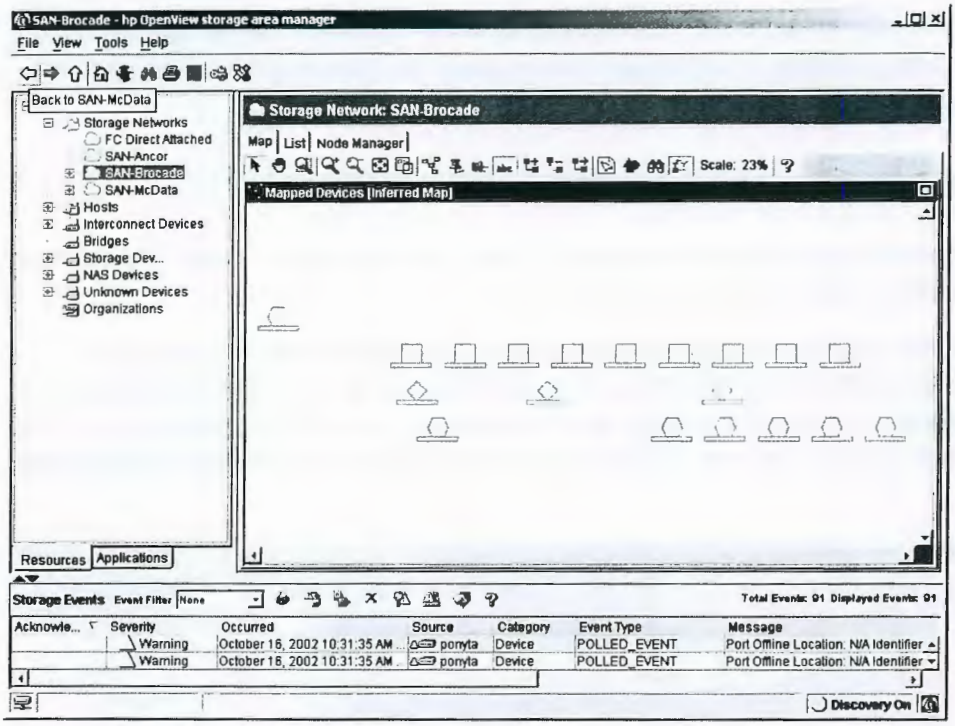
Storage Area Manager provides two device map modes: physical and inferred. The current mode is displayed in a banner at the top of the map.

Devices that appear on physical maps provide enough information that Storage Area Manager is able to establish their identify and connectivity properties. Devices that do not provide sufficient information for Storage Area Map to map them with certainty appear in a node bank at the bottom of the map. Physical maps display physical and user-defined links only.



RQS Nº 03/2005 - CN
CPMI - CORREIOS
0144
Fls: 9
3701
Doc:

Inferred maps display physical and logical devices and all device links together in the same map. Storage Area Manager estimates the connectivity of logical devices by applying its own map rules to the limited information provided by the devices.



You can toggle the currently displayed map between the two modes.

1. Display the device map on which you want to set map mode.
2. Click the **Map Mode** button on the map toolbar to toggle the map between physical and inferred mode.

2.915

Using the layout manager

As Storage Area Manager discovers your storage network, it places devices in device maps. While placing devices in the map, Storage Area Manager also links them using information offered by the devices.

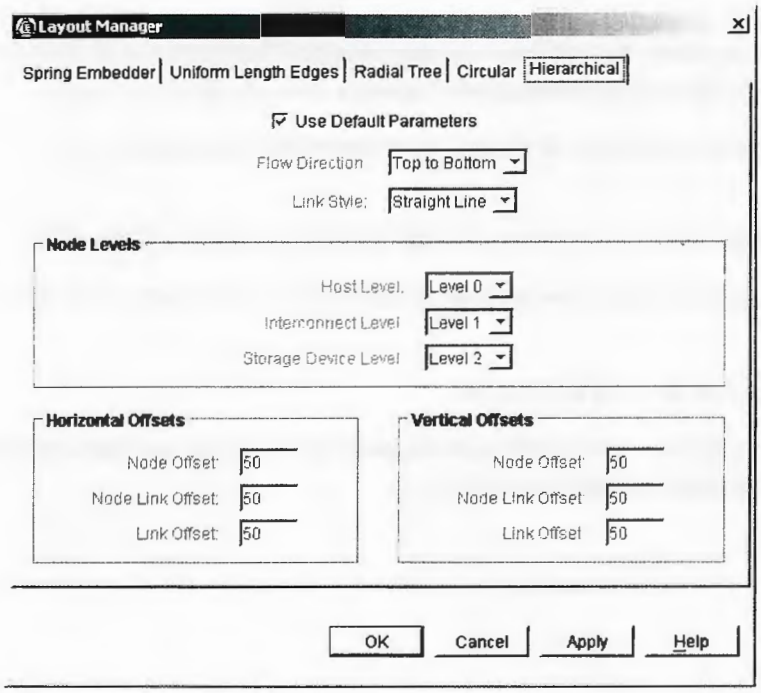
Storage Area Manager uses a default layout when positioning and linking devices; however, the Layout Manager offers additional pre-configured layouts for your device maps:

- **Spring Embedder:** select to position devices in a manner which minimizes link crossings.
- **Uniform Length Edges:** select to position devices so links are of equal length.
- **Radial Tree:** select to position devices in a tree. Branches are determined by device links.
- **Circular:** select to position devices in a circle.
- **Hierarchical:** select to position device types (host, interconnect, and storage) together and in a hierarchy (top-to-bottom, left-to-right, etc.).

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0145
Fls: 11
Doc: 3701

2.914 June

1. Display the map for which you want to change the layout.
2. Click the **Layout Manager** button on the map toolbar. The Layout Manager window appears.



3. Click the appropriate tab for the layout you want.
4. Click the **Apply** button to modify the map.
5. If the map layout is acceptable, click the **OK** button to close the Layout Manager window.

2.913
fune
A.G.

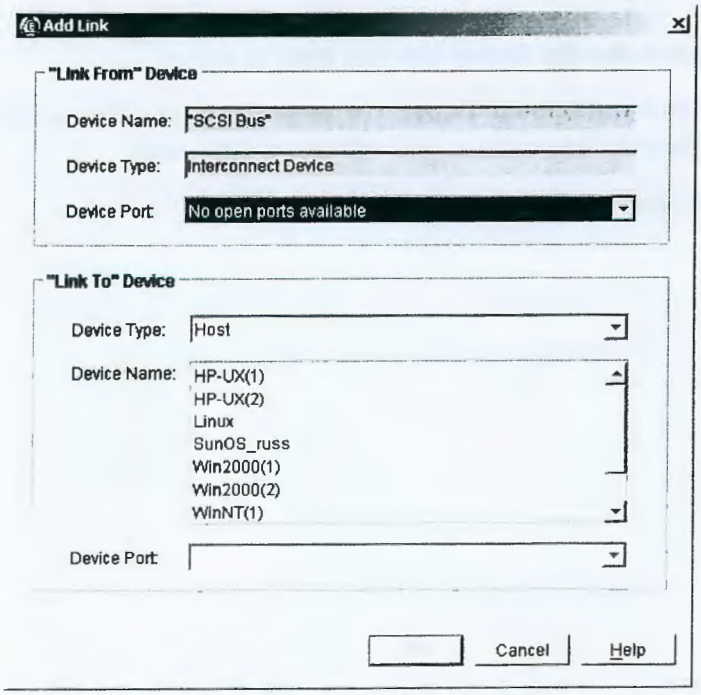
Configuring device links

Upon discovery of the storage network, Storage Area Manager displays the devices it discovers and connects them with either physical or logical links. Device maps include two modes: physical and inferred. Physical map mode displays physical and user-defined links only. Inferred map mode displays all link types.

You can add, move, and remove the links provided by Storage Area Manager.

Adding device links

1. Display the device map which includes the device from which you want to draw the link.
2. Select the icon for the device you want to link to another device.
3. Click the Add Link button on the map toolbar. The Add Link window appears.



4. In the Links From Device section, select the device port from which the link is drawn.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0146
Doc: 3701

2.912
bene

5. In the Links To Device section, select the type of device (host, interconnect, bridge, storage, or unknown) to which you are connecting.
6. Select the device to which the link is connecting.
7. Select the device port to which the link is drawn.
8. Click the **OK** button. A confirmation message appears.
9. Click the **Yes** button to add the device link.

Moving device links

You can only move logical and user-defined links. You cannot move physical links. If you move a logical link, Storage Area Manager redefines it as a user-defined link. However, if the condition that caused the logical link remains, Storage Area Manager returns the logical link as part of the ongoing discovery process.

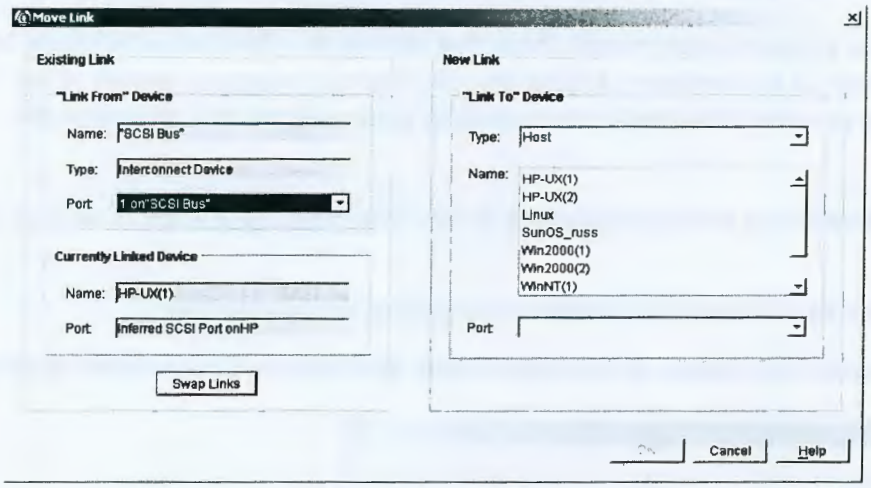
1. Display the device map that includes the device link you want to move.

   When moving links, one "end" of the link will remain the same while the other end is moved. For the next step, select the device icon that will remain the same.

2. Select the device icon that is connected to the link you want to move.

2.911
fls.

3. Click the Move Link button on the map toolbar. The Move Link window appears.



Note You can click the **Swap Links** button to change the "end" of the link that will move. The devices displayed in the Link From Device and Currently Linked boxes will interchange.

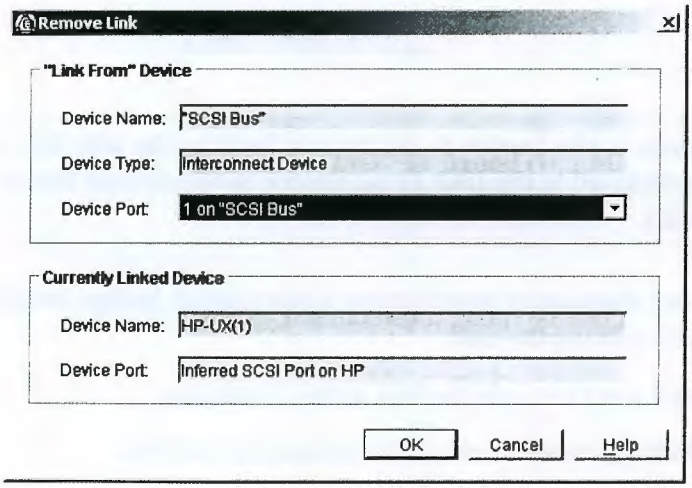
4. In the New Link section, select the type of device (host, interconnect, bridge, storage, or unknown) to which you are moving the link.
5. Select the device to which you want to move the link in the Name box.
6. Select the device port to which you want to move the link in the Port box.
7. Click the **OK** button. A confirmation message appears.
8. Review the information in the message, and click the **Yes** button.

EQS Nº 03/2005 - CN
CPMI - CORREIOS
0147
Fls:
Doc: 3701

Removing device links

You cannot remove physical links (except those that appear in a direct-attached [host to storage device] map). If you remove a logical link, the link may reappear as part of the ongoing discovery process if the factors that resulted in the original link inference still exist.

1. Display the device map which includes the device from which you want to remove the link.
2. Select the icon for the device from which you want to remove the link.
3. Click the Remove Link button on the map toolbar. The Remove Link window appears.



4. In the Links From Device section, select the device port from which you want to remove the link.
5. Verify that you are removing the link you want by reviewing the information in the Currently Linked Device section.
6. Click the **OK** button. A confirmation message appears.
7. Click the **Yes** button if this is the link you want to remove.

2.909
frente

Managing events

As Storage Area Manager monitors the storage network, it displays events in the event panel. Each entry in the event panel displays a corresponding event severity level, the date and time the event occurred, the source of the event, and a brief description of the event. In addition to severity level, events are also defined by their event category.

Once events are displayed in the event panel, Storage Area Manager offers many features that enable you to work with the information displayed.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0148
Fls: 17
Doc: 3701

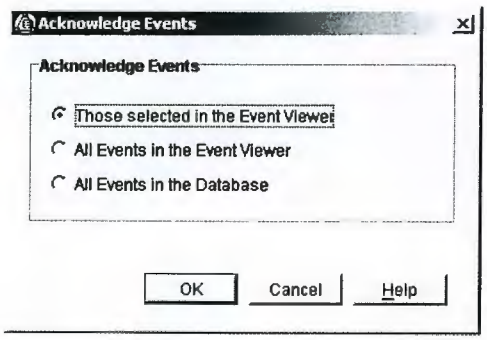
2908
June

Acknowledging events

Storage Area Manager's event management system enables you to acknowledge events that appear in the event panel or are stored in the database.

Note Storage Area Manager may have additional events stored in its database that are not displayed in the event panel. For example, if you apply an event filter to the event panel, then only events meeting the filter's criteria appear in the event panel.

1. If you want to acknowledge only selected events, select the events you want to acknowledge in the event panel.
2. Click the Acknowledge Events button on the event toolbar. The Acknowledge Events window appears.



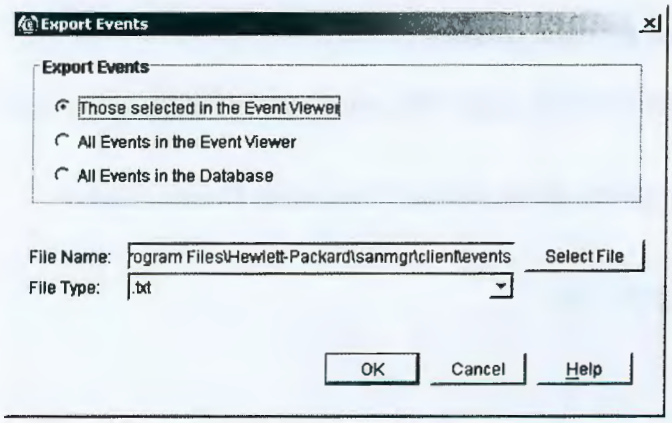
3. Select the appropriate radio button depending on if you want to acknowledge selected events, all events in the event panel, or all events in the database.
4. Click the **OK** button.
5. Verify that the acknowledge event icon appears in the event panel's Acknowledgement column for the appropriate events.

ECT
Q. 907
fune

Exporting events

You can export events to a .txt, .csv, or .xml file. For example, you may want to export events for record-keeping purposes before deleting them from the event panel.

1. If you want to export only selected events, select the events you want to export in the event panel.
2. Click the Export Events button on the event toolbar. The Export Events window appears.



3. Select the appropriate radio button depending on if you want to export selected events, all events in the event panel, or all events in the database.
4. Click the **Select File** button to browse to the location where you want to save the file and to enter a name for the file.
5. Select the file type (.txt, .csv, or .xml) for the exported event file in the File Type box.
6. Click the **OK** button.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0149
Fls:
Doc: 3701

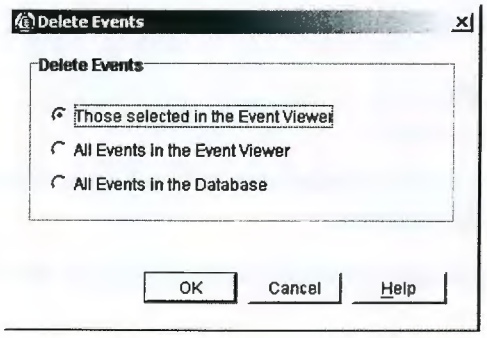
Deleting events

Events are saved in the Storage Area Manager database and contribute significantly to the growing size of the database. In order to manage the number of events in the event panel and the size of the database, you should delete events on a regular basis.

Storage Area Manager offers two methods for deleting events. You can delete events directly from the event panel, or you can configure Storage Area Manager to automatically delete events based on criteria you set.

Deleting events from the event panel

1. If you want to delete only selected events, select the events you want to delete in the event panel.
2. Click the Delete Events button on the event toolbar. The Delete Events window appears.



3. Select the appropriate radio button depending on if you want to delete selected events, all events in the event panel, or all events in the database.
4. Click the **OK** button. A confirmation message appears.
5. Click the **Yes, Delete** button to confirm deletion.

2.905
fls.

Configuring automatic event deletion

You can define rules that Storage Area Manager uses to automatically delete events on an hourly basis. You can define multiple event deletion rules.

For example, you could define a rule to automatically delete all Informational events that are 60 days or older. You could define a second rule to automatically delete all acknowledged events. If an event matches the criteria of either rule, it will be deleted during the next event cleanup cycle.

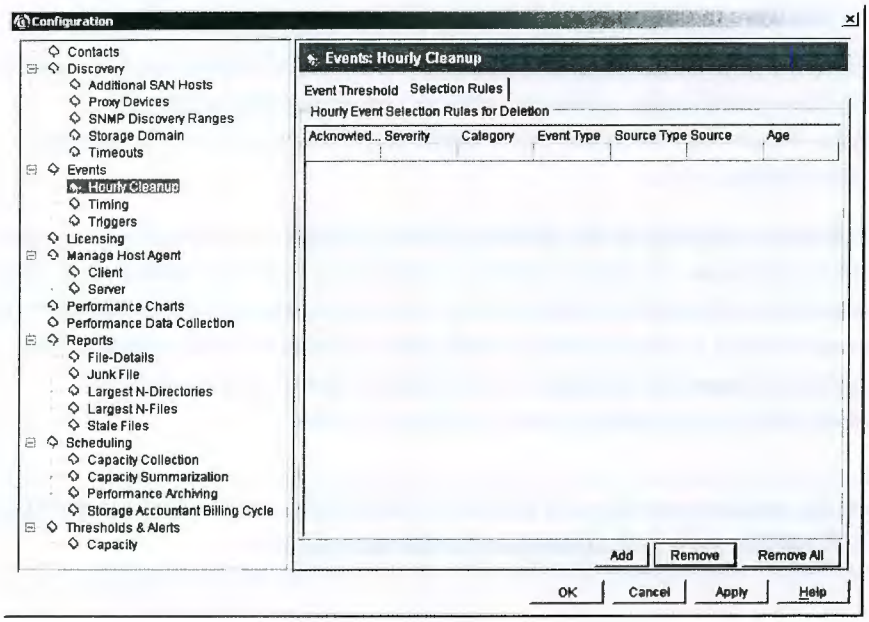
The event cleanup process consists of two phases. If the number of events stored in the database exceeds the maximum number of events threshold, phase 1 is initiated. In this phase, events are automatically deleted based on the criteria set on the Selection Rules tab. If the number of events stored in the database continues to exceed the threshold after phase 1 is complete, then phase 2 is initiated. In this phase, the oldest events are automatically deleted until the maximum event threshold is met.

Note You cannot restore events once they have been deleted. Consider exporting events at regular intervals for record-keeping purposes.

1. From the **Tools** menu, select **Configure**.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0150
Doc: 3701

2. In the Configuration window's navigation tree, expand the **Events** menu, then select **Hourly Cleanup**.



3. Enter the maximum event threshold in the Maximum Number of Events box.
4. Click the **Selection Rules** tab.
5. Click the **Add** button to add a row to the Hourly Event Selection Rules for Deletion table. Each entry represents an event cleanup rule. The cells in each entry define the rule's criteria.

Caution If the table contains a blank row, **all** events are deleted when the hourly cleanup occurs.

6. To define the rule's criteria, click a cell that represents the criteria you want to add, then select the applicable value.

   For example, click the Severity cell, then select the applicable severity level.

2.903
fls

7. Repeat steps 5 and 6 if you want to add another deletion rule to the Hourly Event Selection Rules for Deletion table.
8. Click the **OK** button to save changes and close the window. If the threshold criteria is met, Storage Area Manager performs the cleanup process immediately and then in hourly intervals thereafter.

Adding event filters

Storage Area Manager includes several default event filters to help you manage what you see in the event panel. However, you may want to customize your own event filters. For example, you may want to create an event filter that only displays Critical events for a particular device.

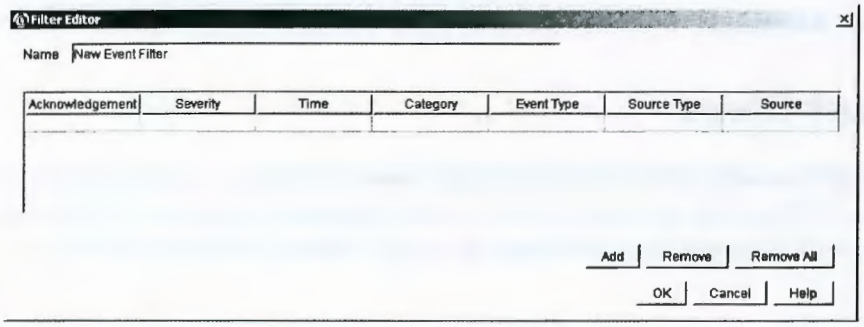
When adding an event filter, each row in the Filter Editor window represents a rule to apply when filtering the event panel. Each rule is defined by a set of criteria. In order for an event to appear in the event panel when this filter is applied, the event must meet all criteria set for a particular rule. For example, if you define an event severity criteria of "Critical" and a source criteria of "Device A", only Critical events for Device A meet the criteria of this rule.

An event filter may also include more than one rule. If an event filter includes more than one rule, then any event that meets the criteria of one or more of the rules will appear in the event panel when this filter is applied. For example, an event filter includes two rules. The first rule defines event severity of Critical as its only criteria. The second rule defines Source criteria of Device A as its only criteria. All events with a Critical event severity and all events from Device A meet the criteria of this event filter.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0151
Fls:
Doc: 3701

C T
2.902
Irene

1. Click the Event Filters button on the event toolbar.
2. Click the **Add** button. The Filter Editor window appears. A row that represents the filter's first rule is automatically added.



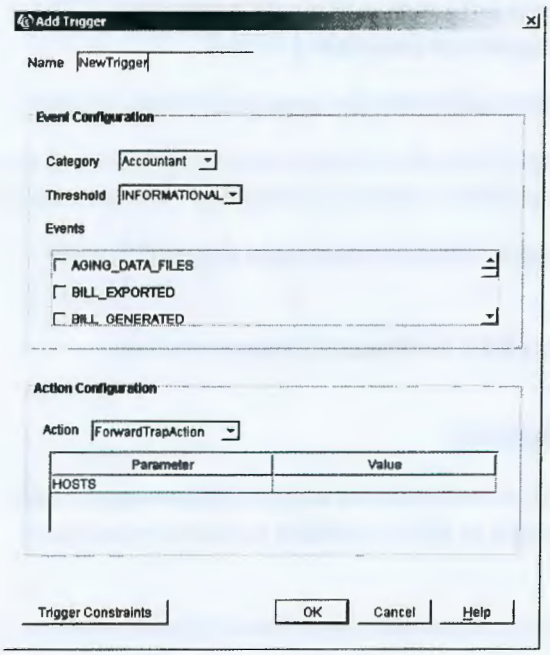
3. Enter a name for this event filter in the Name box.
4. Define the criteria for this event filter by clicking a cell and selecting from the list of options within that cell. For example, click the Severity cell and select the applicable event severity level.
5. Repeat step 4 until you have defined all criteria for this rule (row).
6. Click the **Add** button, and repeat steps 4 and 5 if you want to additional rules to this event filter.
7. Click the **OK** button to save the event filter and close the Filter Editor window.

2.901
fun

Adding event triggers

Event triggers enable you to assign actions to events that meet criteria you specify. Storage Area Manager includes several default event triggers; however, you may want to create additional event triggers that are appropriate for your environment. For example, you can define an event trigger to send e-mail notification to the on-call contact when Critical events occur.

1. Click the Event Triggers button on the event toolbar.
2. Click the **Add** button. The Add Trigger window appears.



3. Enter a name for this event trigger in the Name box. The trigger name may not included white space characters, brackets ({,}), or periods.

   Events are defined by their category (for example, Device), specific type (for example, STATUS_CHANGED_EVENT) and severity level (for example, WARNING). The action defined by this event trigger will initiate when all three event criteria are met.

4. Select the event category you want to include in the Category box.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0152
Fls.
3701
Doc:

5. Select which event severities you want to include in the Threshold box.

   Events for this trigger include the selected severity and above. For example, if you select **INFORMATIONAL**, all event severities are included. However, if you select **MAJOR**, only events with severity levels of Major and Critical are included.

6. Check the checkbox for each event you want to include in the Events box.

   Available events depend on the Category you select. You can check more than one event checkbox.

7. Select which action to initiate for this trigger in the Action box. The parameters displayed in the table below the Action box is based on the action you select. The StoreAction action does not have any parameters associated with it.

8. Click the Value cell next to each Parameter, and enter the appropriate information.

   For example, if you selected ForwardTrapAction in the Action box, click the cell next to HOSTS, and enter the IP address of the host to which you want to forward events.

9. Click the **OK** button to add the event trigger to the list and close the Add Trigger window.

10. Click the **OK** button to save changes and close the Events: Trigger window.

Adding constraints to event triggers

You can constrain an event trigger in order to prevent it from initiating based on certain event criteria. You can also configure exceptions to the constraint based on count and duration of the constraint.

For example, if you configure an event trigger for a source type of interconnect devices, the trigger will initiate for all interconnect devices discovered by Storage Area Manager. However, if you do not want the trigger to act on events contributed by a particular interconnect device (Device A), you could add a constraint that prevents the trigger from acting on events contributed by Device A.

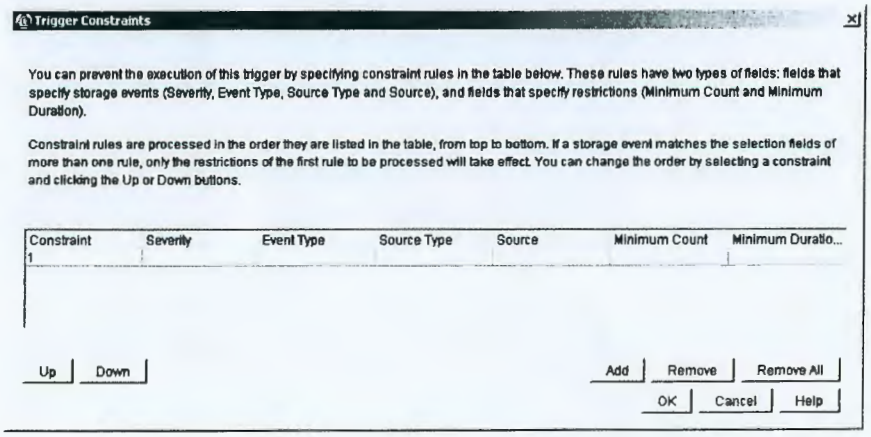
2.899
bene

When adding a constraint, each row in the Trigger Constraints window represents a constraint to apply to the event trigger. Each constraint is defined by a set of criteria. In order for a constraint to take effect, the event that initiated the event trigger must meet all criteria set for the constraint.

An event trigger can include more than one constraint. If a trigger includes more than one constraint, the constraints are applied in the order in which they are listed in the Trigger Constraints window. For example, if an event meets the criteria of two different constraints, the constraint that is listed first in the list is applied

Caution If the first row (rule) in the table is blank and succeeding rows contain rule criteria, this feature interprets the blank row as "always constraint this trigger" and applies it as such. If the first row is blank and no other rows appear for this constraint, then the trigger is not constrained.

1. From the Add Trigger or Edit Trigger window, click the **Trigger Constraints** button. The Trigger Constraints window appears. A row that represents the first constraint is automatically added if the event trigger does not already include a constraint.



2. Click the **Add** button if the table does not already include a blank row.
3. Define the criteria for this constraint by clicking the Severity, Event Type, Source Type, and Source cells and selecting the value you want.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0153
Fls:
Doc: 3701

2.898
Irene

4. If you want to add an exception to this constraint based on the number of times the trigger is constrained, enter a numerical value in the Minimum Count column.

   For example, if the count criteria is 5, the event trigger is constrained the next five times the trigger constraint's criteria is met, initiates the trigger the sixth time the constraint's criteria is met, and then is constrained again for the next five times.

5. If you want to add an exception to this constraint based on how long the trigger is constrained, enter a numerical value (in seconds) in the Minimum Duration column.

   For example, if the duration count is 1800 (30 minutes), the event trigger is constrained for 30 minutes from the time the trigger constraint's criteria is met, initiates the trigger the next time the constraint criteria is met, and then is constrained again for the next 30 minutes.

6. Repeat steps 2 through 5 to add additional rules to this event trigger constraint.

7. Click the **OK** button to add the constraint to the event trigger and close the Trigger Constraints window.

2.897
bene

Managing folders

Storage Area Manager's folder feature enables you add nodes (folders) to the Resources tree and then structure resources under the folder.

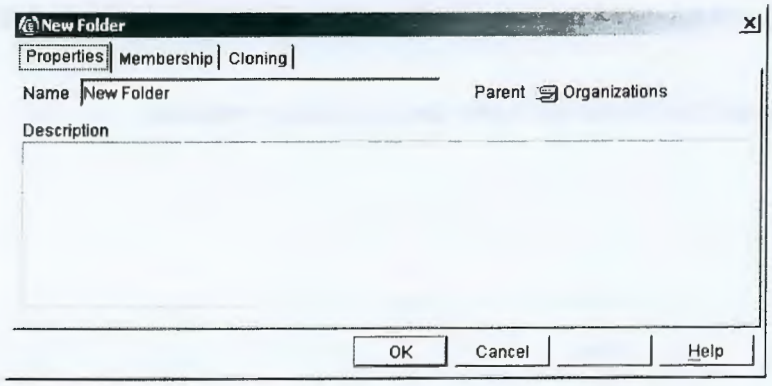
This feature is intended for sizeable storage networks in which many nodes, subnodes, and resources may appear in the Resources tree. You can add a folder to all nodes in the Resources tree except the Domain and Storage Networks nodes. You can also add subfolders under folders that you added previously.

For example, if a storage network contained 100 hosts at three different locations, you could create folders that represent each of the locations and then structure the hosts under the applicable location. When scanning the Resources tree, you would only have to scroll past the three "location" folders rather than all 100 hosts.

A cloning feature enables you to add copies of the folder at the same time you add the original folder. For example, you can create a folder named "Site A" under the Hosts, Interconnect Devices, and Storage Devices node.

Adding folders

1. In the Resources tree, right-click the node or folder under which you want to add a folder, and select **New Folder** from the shortcut menu.



RQS Nº 03/2005 - CN
CPMI - CORREIOS
0154
Fls:
3701
Doc:

2. Enter the folder's name in the Name box.
3. Enter a description for the folder in the Description box.

   If you want to add "clones" of this folder in other Resource tree nodes, continue with step 4. If you want to create this folder only, continue with the next section, "Adding members to folders".
4. Click the **Cloning** tab.
5. Check the **Enable Folder Cloning** checkbox.
6. Check all boxes that represent nodes under which you want to add a clone of this folder.
7. Check the **Replicate Description Fields** checkbox if you want to copy the description you entered on the Properties tab to all cloned folders.

Adding members to folders

1. Click the **Membership** tab.
2. Click the **Add Members** button.
3. Use the Look in drop-down box and Up button to display the node that contains the resource you want to add to the folder's membership.
4. Select the resource you want to add from the Member list. You can select multiple resources.
5. Click the **OK** button to add the resource as a member of the folder and close the Add Members window.
6. Click the **OK** button to add the folder and close the New Folder window.

2.895
Irene

Managing organizations

Organizations enable you to define storage resources as a unique entity. Storage resources can include hosts, bridges, storage devices, interconnect devices, NAS devices, and unknown devices.

Organizations do not necessarily reflect a physical relationship within the storage network. Any storage resource discovered by Storage Area Manager can be added to any organization. A storage resource can be a member of more than one organization.

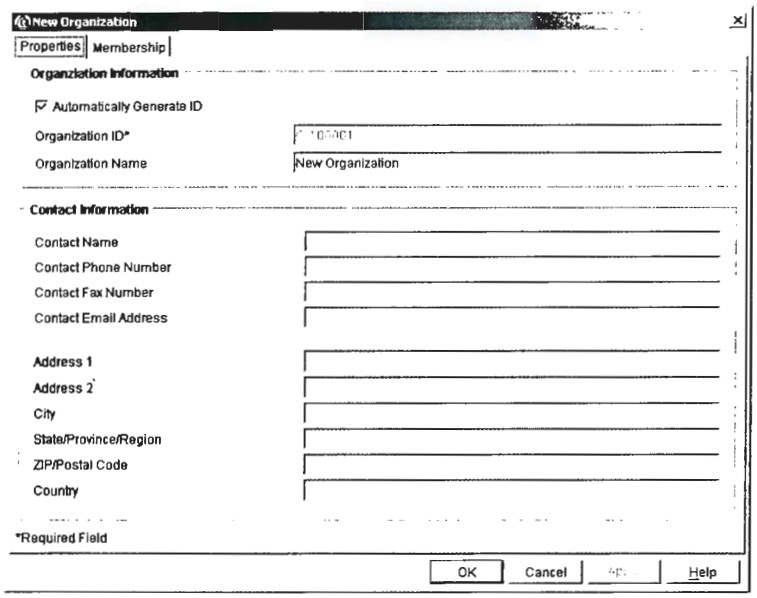
Once an organization's membership is defined, you can use Storage Builder to view capacity data specific to the organization's membership. (Storage Builder must be installed and licensed.)

You can also use Storage Accountant to add accounts to an organization, which enables Storage Accountant to bill for the storage used by the organization's members. (Storage Accountant must be installed and licensed.)

TROS Nº 03/2005 - CN
CPMI - CORREIOS
0155
Doc: 3701

Defining an organization's properties

1. Select the **Organizations** node in the Resources tree to view the Organizations view panel.
2. Click the **New Organization** button. The New Organization window appears.



3. If you want to modify the automatically generated organization ID, uncheck the Automatically Generate ID checkbox, and enter the ID you want in the Organization ID box.
4. Enter a name for this organization in the Organization Name box.
5. Complete the Contact Information section for this organization's primary contact. This is an optional step.

ECT
fls. 893
Rene
CPMI - E

Adding members to the organization

1. Click the **Membership** tab.
2. Click the **Add** button, and select the device type for the storage resource you want to add as a member. The Add Members of type window appears.
3. Select the storage resource you want to add, and click the **OK** button. You can select more than resource at a time.
4. Repeat steps 2 and 3 until all the members you want to add to this organization are displayed on the Membership tab.
5. Click the **OK** button to add the organization and close the window.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0156
Fls: 33
Doc: 3701

2.892
June

Implementing in cluster environments

Refer to the following subsection when implementing Storage Area Manager in MSCluster and AIX cluster environments.

Implementing in MSCluster environments

1. Install MS Cluster on both Windows 2000 management servers (servers A and B).
2. Format a share disk for both servers.
3. Install Storage Area Manager 3.0 onto the share disk server A (server B pause). See the *hp OpenView storage area manager 3.0 installation guide* for complete instructions on installing Storage Area Manager.
4. Start MSCluster Admin.
5. Select **Disk Group**, right-click the **Share** disk, then select **move group** from the shortcut menu.
6. Install Storage Area Manager 3.0 onto the share disk of server B.

Note Storage Area Manager must be installed in the same directory on server B as it is on server A.

7. Use MSCluster Admin to create general service resources for Storage Area Manager's services, including:
   - HP OpenView SAM Bridge
   - HP OpenView SAM Embedded DB
   - HP OpenView SAM ManagementServer
8. Start Storage Area Manager on server B.

ECT
2.891
fls
Cpl - A

9. Change the Network Order Binding to use LAN connection before private connection on server A and server B.
   a. From the Windows Start menu, select **Settings**, then select **Control Panel**.
   b. Double-click **Network and Dial-up Connections**.
   c. From the **Advanced** menu, select **Advanced Settings**.
   d. On the Adapters and Bridge tab, ensure that Local Area Connection is listed first in the Connections box.
10. In MSCluster Admin, bring on the general services you created in step 7.
11. Remotely install the Storage Area Manager Host Agent software to each SAN host.
12. Fail over to server A.
13. Start Storage Area Manager on server A.
14. From the **Tools** menu, select **Manage Host Agent**, then select **Update Host Agent Access**.
15. Select all hosts in the managed host list, and click the **Update Access on Selected Hosts** button.

    All hosts should now appear under the Hosts node in the Resources tree.

RQS Nº 03/2005 - CN
CPML - CORREIOS
0157
Fls:
Doc: 3701

How hp OpenView storage area manager operates in AIX cluster environments

Requirements

Storage Area Manager requires the following to operate in a cluster environment.

- Each host in the cluster must have one static, non-migrating IP address.
- The IP Address must be accessible by the Storage Area Manager management server.

These requirements necessitate that each AIX host contain a minimum of two and possibly three NIC cards.

Description

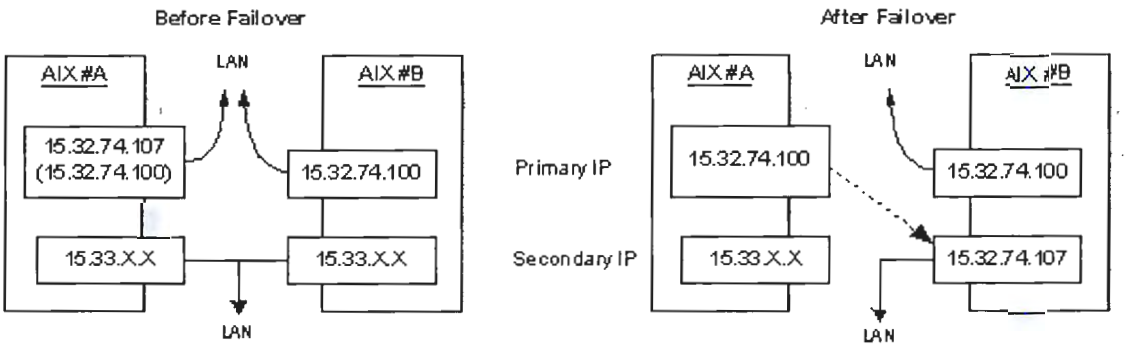


Figure 1 AIX cluster example

From Storage Area Manager's perspective, an AIX cluster is a group of hosts with each host containing a floating IP address in addition to its static IP address. One host in the cluster is a master for the clustered resource. In this example, AIX #A is the master with floating IP address 15.32.74.107.

In addition, AIX clusters require a heartbeat to be transmitted between hosts (illustrated by IP address 15.33.X.X). This heartbeat can be sent by serial connection although that is not recommended.

ECT
2.889
fls.
CPI-AC

Failover

During a failover, the floating IP address assumes ownership of a NIC card, which hides the consumed IP address and exposes the old NIC card's IP address on the host that failed (after it is rebooted).

In figure 1, the IP address 15.32.74.100 is not accessible to Storage Area Manager until after failover and the subsequent reboot occur, at which time the floating address migration enables the old IP address to resume ownership of the NIC card.

This example reflects a single resource failover. In some environments, multiple resources may be simultaneously monitored (for example, a web server on AIX #A and a database on AIX #B). In these configurations, each host acts as a primary and secondary for its peer. Failover can potentially occur in either direction.

Recommendation

In order for the cluster illustrated in figure 1 to satisfy Storage Area Manager's cluster requirements, we recommend that a separate NIC be supplied, which cannot be a failover candidate.

Add the IP address of this separate NIC to the AIX host's commIpAddr.txt file, which is located in the /etc/opt/sanmgr/hostagent/config directory. Storage Area Manager will then identify each host by this new, non-migrating IP address.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0158
Fls: 37
Doc: 3701

2 STORAGE ACCOUNTANT

hp OpenView storage accountant features

Billing basics

Getting started with billing

Service level setup and administration

Account setup and administration

Billing configuration

Billing data archiving

Setting currency preferences

Integrating bills with other applications

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0159
Fls: 3701
Doc:

2.887
bene

hp OpenView storage accountant features

Storage Accountant meters storage space in organization accounts and reports the associated cost at the end of each month. Accounts belong to internal or external organizations. You must install and license Storage Accountant to use its features.

Storage Accountant adds the following features to Storage Area Manager:

- Monthly and interim bill reports. Storage Accountant rolls up daily charges into a monthly bill that is arranged by organization and account. Detailed bills describe the charges for each LUN. Summary bills show only the total charges for each organization and account. Using the Bill Viewer, you can view, export, and print bills for the current (interim) or past billing periods and for all or individual organizations.
- Storage device and service level billing reports. Storage Accountant creates monthly billing reports that are organized by storage device or service level. Summary reports show the total charges for the storage device or service level LUNs in accounts and LUNs not in accounts. Detailed reports show summary information and a LUN-by-LUN description of charges.
- High-level statistics in the Reports tab of the Accountant Home view panel. This view panel allows you to view reports and bill generation information and to configure the billing period.
- Centralized setup functions in the Accounting tab of the Accountant view panel. This view panel provides all the tools you need to set up storage billing. In the Accounting tab, you can click icons to view, create, and add LUNs to service levels; view and create organizations; add organization accounts; and attach LUNs to accounts. You can also view the total number of service levels, organizations, LUNs in service levels, and total storage value that is billed and not billed.
- Service Level, Organization and Account nodes in the Resources tree. Storage Accountant associates LUNs with service levels and then associates the service-rated LUNs with organization accounts. You can view, create, add LUNs to, and maintain service levels and organization accounts from these nodes.

ECT
2.886
Fls.
CPMI - AV

- Audit log of billing transactions and LUN events. A quick look at the audit log will tell you when changes were made to organizations, accounts, service levels, or the billing schedule; if daily usage is being regularly collected; when bills were generated and exported; and if a LUN's status changed. The Audit Log Viewer lets you view, export, and print the audit log.
- Accountant scheduler. The Storage Accountant billing cycle scheduler in the Configuration window lets you specify when the monthly bill is generated, when old bills and audit entries are deleted, and the format and location of exported files.
- CLUI commands. You can use the CLUI to expedite most of the tasks that you can perform in the graphical user interface; for example, adding LUNs to service levels or accounts, creating organizations, removing LUNs from service levels, and generating bills.
- Integration with HP OpenView Internet Usage Manager (IUM). Storage Accountant outputs LUN state data on a monthly basis. This data can then be incorporated into IUM. To enable this functionality, a Hewlett-Packard support representative must complete the integration procedure.
- Exported bills in CSV, HTML, and XML format. Storage Accountant automatically exports monthly bill reports in a format and location that you choose. You can set event triggers that launch a third-party billing application once the report is exported. The details that you need to integrate Storage Accountant bills with other applications are provided in the hp OpenView storage area manager administrator's guide and in Storage Area Manager's document directory (.\client\doc\export_files).
- Monthly and interim bill reports. Storage Accountant rolls up daily charges into a monthly bill that is arranged by organization and account. Detailed bills describe the charges for each LUN. Summary bills show only the total charges for each organization and account. Using the Bill Viewer, you can view, export, and print bills for the current (interim) or past billing periods and for all or individual organizations.

ROS Nº 03/2005 - CN
CPMI - CORREIOS
0160
Fls:
Doc: 3701

Billing basics

Bills are summaries of storage charges to organizations. Bills are produced in two formats:

- Text that is displayed in the Bill Viewer window
- An exportable file that is automatically saved at the end of each billing period

How charges are calculated

Storage Accountant charges are based on the size and price of the LUNs that a Storage Accountant user attaches to an organization's accounts. The price of a LUN depends on its associated service level. The amount charged in a monthly bill is the product of the LUN size and price per GB per hour and the number of hours that the LUN belonged to the account during the billing period.

Charge = LUN size in gigabytes (GB) x price per GB per hour x hours

For example, if organization A has an account with an attached 9-GB LUN whose price is 5 cents per GB per hour, the charge after 20 hours would be 9 GB x $.05/GB/hour x 20 hours, or $9.00.

Storage Accountant records day-to-day changes in the factors that make up the charge and sums up the charges at the end of the billing period.

How charges become bills

At the end of each day, Storage Accountant records all of the day's transactions that affect storage charges; for example, a LUN is added or removed from an account, the service level price is changed, or the LUN is resized. Once a month, these daily records are compiled into a single binary file of usage information, such as LUN 01 used by Account AA from October 1, 2001, 09:27:54, to October 30, 2001, 23:59:59, at a price of $.07/GB/hr. The information in this file is sorted by organization and account to display requested bills in the Bill Viewer and to produce specially formatted files that can be imported by a third-party billing application.

ECT 2.884 Bune

Getting started with billing

Before Storage Accountant can produce bills, you must set up service levels and customer accounts and assign LUNs to them. Figure 2 illustrates the setup steps.

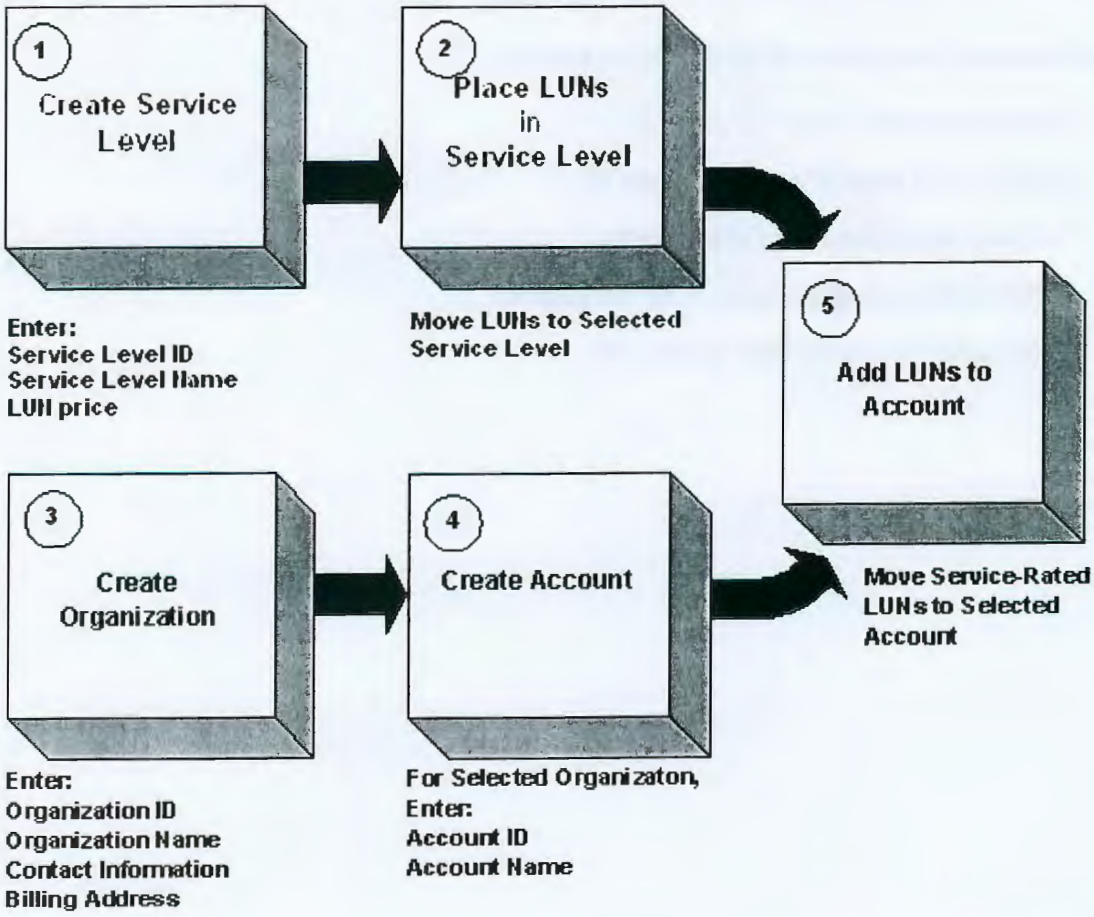


Figure 2 Setting up storage accountant

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0161
Fls:
Doc: 3701

2.883
Irene

The arrows in figure 2 indicate necessary sequences. For example, you cannot place LUNs in a service level (step 2) until you create a service level (step 1). Most importantly, you cannot add LUNs to accounts (step 5) until you have completed all the other actions (1, 2, 3, and 4).

Note You do not need to create the organization (step 3) if it already exists in Storage Area Manager.

See the instructions for each setup step as follows:

1. "Creating service levels" on page 45.
2. "Setting LUN service levels" on page 45.
3. "Adding organizations" in online Help.
4. "Adding accounts to organizations" on page 48.
5. "Adding LUNs to accounts" on page 49.

2.882
bene

Service level setup and administration

Service levels determine the price that will be charged for LUN use and typically reflect the relative value of the LUN or LUN service. You need to create service levels and assign LUNs to them so that Storage Accountant can charge for their use.

Creating service levels

Use this procedure to define a service level that you will later associate with specific LUNs.

1. In the Applications tree, expand **Storage Accountant**.
2. Right-click **Service Levels** and select **New Service Level**.
3. Enter data in the New Service Level boxes. Required fields are marked with an asterisk (*).

   For quick entry, accept the automatically generated identifier and enter the service level name and LUN price/GB/hour. Service Level Description is optional.
4. Click **OK** to save the changes and close the window. The new service level appears in the Service Levels view panel and under **Service Levels** in the Applications tree.

The next step is to set LUN service levels.

Setting LUN service levels

Use this procedure to place LUNs in a specified service level. The procedure treats the service level like a bucket that LUNs are added to or removed from. The service level must be previously defined (see "Creating service levels").

1. In the Applications tree, expand **Storage Accountant** and **Service Levels** to reveal the specific service level.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0162
Fls:
3701
Doc:

2. Right-click the service level and select **Add/Remove LUNs** from the shortcut menu. A new window lists all LUNs without a service level on the left and all LUNs that are already associated with the selected service level (but not yet attached to an account) on the right.

Note To select LUNs from a particular storage device, select the device name in the Select Source of LUNs list on the left side of the view panel. Only the LUNs that are in the selected storage device are listed.

3. In the list of LUNs without service levels, select the LUNs that you want to place in this service level and click the **Add** button. The selected LUNs are dimmed in the list on the left and added in blue to the Add List on the right. A green arrow appears in the column beside the moved LUNs in each list, indicating that the addition is pending.

   You can continue selecting LUNs and clicking **Add**. You can also select and remove LUNs from the list on the right. All actions remain pending until you click the **Apply** or **OK** button.

Note Moving large numbers of LUNs will increase the time it takes to apply the changes, about a minute for every 2000 LUNs. During this time, a message window shows the progress of the changes. There is a short delay before the view panel is updated with the changes.

Note For best performance, HP recommends limiting the total number of LUNs in a service level to 2000. If you have more than 2000 LUNs that need to use the same price, you can create an alternate service level with the same price.

4. Click **OK** to save the LUN placements and close the window.

2.880

Deleting service levels

Use this procedure to discontinue an obsolete service level. Any LUNs in the service level will be freed for placement in other service levels. Affected LUNs must be removed from accounts before the service level can be deleted. You cannot delete a service level that has LUNs in use.

1. In the Applications tree, expand **Storage Accountant** and **Service Levels** to reveal the specific service level.
2. If the service level contains LUNs that are in use, remove the LUNs from the accounts that are using them (see page 50).
3. Right-click the service level and select **Delete** from the shortcut menu. A confirmation window shows the name of the service level, the number of affected accounts, and the number of LUNs that will be freed by deleting the service level.
4. Click **OK** to delete the service level and close the window. The service level no longer appears in the Applications tree or the Service Levels view panel.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0163
Fls: 47
Doc: 3701

Q.879 Front

Account setup and administration

Storage is billed by the accounts that belong to organizations. An organization can have many accounts, but must have at least one account to accumulate storage charges.

Adding accounts to organizations

Use this procedure to define an account for an existing organization. If you need to create the organization, complete the procedure "Adding organizations," described in online Help, and then return to this procedure.

1. In the Resources tree, expand **Organizations.**
2. Right-click the organization name and select **New Account** from the shortcut menu. A New Account window shows the organization ID and name and provides places to enter account information. The only required information is the account ID, which Storage Accountant generates for you.
3. If you want to change the automatically generated account ID, clear the **Automatically Generate ID** check box and enter the desired ID in the corresponding text box. The ID must be unique among all accounts in the storage domain.
4. Optionally, enter a name for the account. Account names must be unique within the organization. If you do not enter a name, the account will be identified in the Resources tree by its ID.
5. Click **OK** to add the account and close the window. The new account appears under its respective organization in the Resources tree and in the Accounting tab of the Organizations view panel.

Note The organization will not be charged until you attach LUNs to one of its accounts.

E C T
2.878
- AC

Adding LUNs to accounts

Use this procedure to attach LUNs to an account. If the LUNs are not already attached to a service level, complete the procedure "Setting LUN service levels," described on page 45, and then return to this procedure.

Caution Make sure that LUNs are physically and logically accessible to the organization before you add them to an account. Otherwise, organizations can be charged for LUNs that they cannot use.

1. In the Resources tree, expand **Organizations** and the individual organization that owns the desired account.
2. Right-click the specific account and select **Add/Remove LUNs** from the shortcut menu. A new window lists all available LUNs on the left and all LUNs that are already attached to the account on the right.

Note To select LUNs from a particular storage device or service level, select **Storage Devices** or **Service Levels** in the top box in the left panel. The contents of the second box change accordingly. When you select a specific storage device or service level from the second box, the list of available LUNs will show only the LUNs in that device or service level.

3. In the left box, select the LUN(s) that you want to assign to the selected account and click the **Add** button. The selected LUNs are dimmed in the list on the left and added in blue to the Add List on the right. A green arrow appears in the Status column beside the moved LUNs in each list, indicating that the addition is pending.

   You can continue selecting LUNs and clicking **Add**. You can also select and remove LUNs from the list on the right. All actions remain pending until you click the **Apply** or **OK** button.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0164
Fls:
3701
Doc:

Note Moving large numbers of LUNs will increase the time it takes to apply the changes, about a minute for every 2000 LUNs. During this time, a message window shows the progress of the changes. There will be a short delay before the view panel is updated with the changes.

For best performance, HP recommends limiting the total number of LUNs in an account to 2000. If you want to assign more than 2000 LUNs to the same organization, assign the LUNs to multiple accounts, and then assign the accounts to the organization.

4. Click **OK** to save the LUN placements and close the window.

Removing LUNs from accounts

Use this procedure to discontinue billing for specific LUNs. Billed hours will stop accumulating at the moment that the LUNs are removed, and the LUNs will be freed for use by other accounts.

1. In the Resources tree, expand **Organizations** and the individual organization that owns the desired account.
2. Right-click the account name and select **Add/Remove LUNs** from the shortcut menu. A new window lists all unattached LUNs on the left and, on the right, all LUNs that are currently attached to the selected account.
3. In the list of LUNs in the account, select the LUN(s) to be removed from the account.
4. Click the **Remove** button. The selected LUNs are dimmed in the list on the right and added in blue to the Remove List on the left. A green left arrow appears in the column beside the moved LUNs in each list, indicating that the removal is pending.

   You can continue selecting LUNs and clicking **Remove**. You can also select and add LUNs from the list on the left. All actions remain pending until you click the **Apply** or **OK** button.

2.876

Note Moving large numbers of LUNs will increase the time it takes to apply the changes, about a minute for every 2000 LUNs. During this time, a message window shows the progress of the changes. There will be a short delay before the view panel is updated with the changes.

5. To save the LUN placements and close the window, click **OK**.

Closing accounts

Use this procedure to discontinue billing for a specified account. Charges will be billed up to the moment that the account is closed. The account will be removed from the Resources tree, and attached LUNs will be automatically freed when the account is closed.

Note Although closed accounts are not deleted from the database, they cannot be reopened. To restore an account, you need to add a new account. Because closed accounts are not deleted, their IDs cannot be reused.

1. In the Resources tree, expand **Organizations** and the individual organization that owns the account.
2. Right-click the name of the account and select **Close** on the shortcut menu. A confirmation window shows the name of the account and the number of LUNs that will be freed by closing the account.
3. Click **OK** to close the account and close the window. The account no longer appears in the Resources tree or the organization's view panel.

Note You can view closed accounts by selecting **Show All Accounts** or **Show Closed Accounts Only** from the Select View box in the view panel for an individual organization.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0165
Fls:
Doc: 3701

Billing configuration

Billing occurs on a monthly cycle. The billing period starts on the day and hour that a bill is generated for the previous period. The period ends a month later. For example, a bill is generated on June 28 at 23:00 for the period that ended on June 28 at 23:00, and the bill for the new period, June 28 (23:00) through July 28 (23:00), will be generated on July 28 at 23:00. The billing period is the same for all organizations. You can change the billing period.

When bills are generated, copies are automatically exported to a special location for access by a third-party billing application. You can change the format and location of these files to accommodate your billing application. Storage Accountant does not monitor the export directory, so you may want to set up your own procedures for aging and purging these files.

You can set an event trigger that launches a billing application when Storage Accountant bills are generated. Instructions are on page 54.

Setting the billing period

Use this procedure to specify the day and hour that Storage Accountant generates bills and begins a new billing period.

1. Select **Configure** from the **Tools** menu. The Configuration window opens.

Note You can also open the Configuration window from the Storage Accountant Reports view panel.

2. Find **Scheduling** in the Configuration tree and select **Storage Accountant Billing Cycle**.
3. In the Generate bill on box, enter the day of the month that the bill will be generated; for example, 5. The number must be between 1 and 31. The default day is 1, the first day of the month.

ECT
2.874
fls
CPMI - AC

Note If you choose 29, 30, or 31 as the day of the month to generate a bill, during months that have fewer than 29, 30, or 31 days, the bill will be generated on the last day of the month.

4. In the Generate bill at box, enter the time of day (hh:mm) that the bill will be generated; for example, 22:30 (10:30 pm). The default time is 01:30 (1:30 am).

   Text below the editable boxes shows you the date and time that the next bill will be generated and the duration of the next billing period.

5. Click **OK** to save the changes and close the window.

Setting export options

Use this procedure to specify the file format and location for bills that you want to import into a third-party billing application.

1. Select **Configure** from the **Tools** menu.

Note You can also open the Storage Accountant Configuration window from the Storage Accountant Reports view panel.

2. Find **Scheduling** in the Configuration tree and select **Storage Accountant Billing Cycle**.
3. In the Bill Export section of the Configuration window, select **CSV**, **HTML**, and/or **XML** for the Exporter Output Formats. CSV and HTML are selected by default.
4. For Exporter Output Directory, enter the name of the directory where export files will be stored. The default location is <install directory>\managementserver\data\accountant\exporter\reports.
5. Click **OK** to save the changes and close the window.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0166
Fls:
Doc: 3701

Setting a billing event trigger

After a bill has been generated and exported into the specified directory, an event is generated and recorded in the audit log. This event can be associated with a trigger that will invoke a script to import the newly generated bill into a third-party application. To set this trigger:

1. From the **Tools** menu, select **Configure**.
2. Select **Triggers** under **Events** in the Configuration tree.
3. Click the **Add** button.
4. Enter a name for the event trigger in the Name box. The name cannot include spaces.
5. Select **Storage Accountant** in the Category box.
6. Select **Informational** in the Threshold box.
7. Select **Bill_Exported** in the Events list.

Caution Do not select Bill_Generated, because this event is generated at the beginning of bill generation, and an incomplete or corrupt bill could be imported.

8. Select **Run Command Action** in the Action box.
9. Select **COMMAND** in the Parameter list.
10. Enter a command (including the path) in the Value box next to the COMMAND parameter, for example:
    C:\script.cmd
11. Click the **OK** button to add the trigger to the list and close the Add Trigger window.
12. Click **OK** to save the changes and close the Configuration window.

F C T
2872
fls.

Billing data archiving

Billing data includes bills and the Storage Accountant audit log. The audit log is a record of all billing transactions and system events that affect storage charges. It can help you identify the source of changes or problems in organizations' bills. (See "Viewing the audit log in online Help.) All this billing data accumulates over the months in a growing database. To control the size of the database, Storage Accountant deletes bills and audit log entries that have reached a specified age. You can specify the maximum age of bills and audit log entries according to your priorities for the availability of data versus storage space.

If you need permanent billing records, see "Archiving and restoring bills" on page 56.

Setting the bill retention period

Use this procedure to specify how long bills are kept. Bills are deleted at the end of the next billing period after the specified retention period. Until they are deleted, past bills can be viewed in the Bill Viewer.

1. Select **Configure** from the **Tools** menu.

Note You can also open the Configuration window from the Storage Accountant Reports view panel.

2. Select **Storage Accountant Billing Cycle** under **Scheduling** in the Configuration tree.
3. In the Data Retention section, enter the number of days that you want to keep the monthly bills. The default is 365 days.

Note The audit log lists the files that are purged and the files that will be purged with the next bill.

4. Click **OK** to save the changes and close the window.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0167
Fls:
3701
Doc:

Setting the audit retention period

Use this procedure to specify the maximum age of entries in Storage Accountant's audit log. Entries older than the days specified are automatically deleted from the log.

1. Select **Configure** from the **Tools** menu.

Note You can also open the Configuration window from the Storage Accountant Reports view panel.

2. Find **Scheduling** in the Configuration tree and select **Storage Accountant Billing Cycle**.
3. In the Purge audit log records older than box, enter the number of days that you want to keep entries in the audit log. The default is 365 days.
4. Click **OK** to save the changes and close the window.

Archiving and restoring bills

Use this procedure to make duplicate monthly bills that you can save indefinitely and restore when needed. When you restore a bill that you have archived, you can view, print, or export it just like any other bill.

To archive monthly bills

Once a month, copy the entire contents or just the newest file from the <installdirectory>\managementserver\data\accountant\exporter directory to a secure backup location. Files are named with the start and end times of the billing period separated by an underscore (_); for example, 20010201230000_20010228230000.xml for the month of February 2001.

Note The audit log lists the files that are deleted and the files that will be deleted with the next bill.

ECT 2870 fls

To restore an archived bill to Storage Accountant

1. Copy the desired file from its backup location to <install directory>\managementserver\data\accountant\exporter on the management server. See "File name format" to identify the file for the specified billing period.
2. Execute the CLUI command or open the Bill Viewer to view the restored file. The billing period of the restored file will appear in the Billing Period list.

Note If a restored file is older than Storage Accountant's bill retention period, the file will be deleted when the next bill is generated.

File name format

Bill file names are the times of the first and last daily records that are summarized in the monthly bill. If bills are generated on the first day of the month at 01:00 and daily records are created at 23:00, the bill will include records from the first through the last day of the previous month. Times are specified by year, month, day, hour, minute, and second, and separated by an underscore ("_"), as shown below:

`<yyyymmddhhmmss_yyyymmddhhmmss>.xml`

Where *yyyy* is the year

mm is the month

dd is the day

hh is the hour

mm is the minute

ss is the second

For example, the file corresponding to the billing period January 1, 2001, through January 31, 2001, is named 20010101230000_20010131230000.xml.

The file extension is XML for internal billing files and CSV, HTML, or XML for exported files.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0168
Fls: 3701
Doc:

Setting currency preferences

Use this procedure to change the default settings for the number of digits shown to the right of the decimal place in the Accountant user interface. You can change the display settings for cost per hour totals of billed and unbilled storage, service level price, and cost per hour of individual LUNs.

Note The currency settings in this window apply only to the user interface, and do not affect billing calculations or the Bill Viewer.

1. In the Applications tree, select **Storage Accountant** and click the **Accounting** tab.
2. Click the **Configure number of currency digits** button.
3. Use the drop-down lists to specify the number of digits displayed for total costs per hour billed and unbilled, service level price, and cost per hour for individual LUNs.
4. Click **OK** to apply the changes and close the window.

2868
fune

Integrating bills with other applications

Use this procedure to integrate HP OpenView Storage Accountant with a billing application that produces finished customer statements.

1. Set Storage Accountant's export options to the file format and directory location that your billing application will use. See "Setting export options" on page 53.
2. Set up the billing application to retrieve the current bill file from the export location. See "File name format" on page 57 for the bill naming convention.

Note Consider using Storage Area Manager events and action triggers to start up your billing application as soon as Storage Accountant generates the monthly bill. See "Setting a billing event trigger" on page 54.

3. Map billing application fields to the Storage Accountant export file. Although contents vary depending on the format (CSV, HTML, or XML), all export files contain the following information for each active organization:
   - Unique organization identifier
   - Unique account identifier
   - Size of each billed LUN (in GBs)
   - Price of each billed LUN per GB per hour
   - Total charge for each billed LUN
   - Total charge for each account
   - Total organization charge

See the complete specifications for CSV and XML files in "Integrating hp OpenView storage accountant 3.0 with third-party billing applications" (ThirdParty_Billing.pdf). This document and sample CSV and XML files are located in ./client/doc/export_files (where "." represents the directory where Storage Area Manager is installed).

ROS Nº 03/2005 - CN
CPMI - CORREIOS
0169
Fls:
3701
Doc:

ECT
2867
fun
CPMI

3 STORAGE BUILDER

hp OpenView storage builder features

Physical and logical space

Capacity data collection

Capacity data archiving

Managed directories

Capacity thresholds

Capacity reports

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0170
Fls: 61
3701
Doc:

hp OpenView storage builder features

Storage Builder monitors and reports storage capacity in a storage network. It routinely discovers the physical capacity of storage devices and the logical capacity of hosts and NAS devices, and analyzes the information for current usage, past and future usage trends, and threshold notification. You must install and license Storage Builder to use these features.

Storage Builder adds the following features to Storage Area Manager:

- Capacity views of hosts, NAS devices, storage devices, and the domain. For hosts and NAS devices, view panels show used and free file space. For storage devices, view panels show the disk space that is visible to hosts, still unformatted, and spent in overhead.
- Lists of directories, disks, users, volumes, and volume groups on each host. Click any of these labels in the Resources tree to view corresponding capacity data, including file system and logical volume metrics. Select a specific resource to view more information about the individual directory, disk, user, volume, and so on.
- Correlated views of physical and logical space. At the storage device view, you can see how LUN space is distributed to hosts and volumes. At the host view, you can see the LUNs where volumes reside. When logical volume managers are present or when HP-UX volumes map directly to LUNs, a graphical map shows the relationships between volumes and LUNs.
- Past and future usage trends. Click the graph button in Capacity view panels to view a line graph of past and future capacity. Storage Builder predicts future capacity by identifying trends in past capacity. You can turn this feature on or off, and you can select from a wide range of predictive models.
- Capacity thresholds and threshold events. Storage Builder monitors the current and predicted capacity of individual resources for capacity thresholds. If measured capacity exceeds or falls below a specified limit, Storage Builder sends a threshold notification to Storage Area Manager's event panel. Administrators can set thresholds and configure event triggers.

E C T
2859
fls
CPI - AC

4. Click the **Start Collection** button.
5. In the Start Hostagent Data Collection window, select one or more types of data to collect: **Volume Data**, **File Data**, and/or **User Data**.
6. Click **OK** to start collecting the selected capacity data on the selected host(s).

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0371
Fls:
Doc: 3701

Capacity data archiving

Storage Builder routinely summarizes the data that has been collected over several days and then discards the original data. Summaries contain the weighted average, minimum and maximum values, and standard deviation for each measurement that Storage Builder collects. These values enable Storage Builder to display capacity history, predict future capacity, and conserve space in the database.

Summarized data is saved for as long as you want to view historical data, or as long as there is space for the growing database.

Scheduling capacity summaries

Use this procedure to set the schedule for summarizing collected capacity data and for deleting aged summaries. The procedure displays the Configuration window with the current summarization settings in editable text boxes.

1. Select **Configure** from the **Tools** menu.
2. Select **Capacity Summarization** under **Scheduling** in the Configuration tree.
3. To change the minimum number of days that data is kept before it can be summarized, enter a value for Accept measurements for summary after ___ days. Higher values increase the time that unsummarized data is displayed in capacity graphs. The default is 7 days. Collected data is deleted after it is summarized.
4. To change the number of days of collected data that summaries include, enter a value for Summarize collected measurements every ___ days. Higher values increase the interval between summaries in capacity graphs. The default is 7 days.

Note Higher summary intervals also affect the period for which unsummarized data is displayed in capacity graphs. For example, if data must be kept 7 days before it can be summarized and summaries occur every 5 days, some data will be 12 days old before it is summarized.

2857
June
CPI-AC

5. To increase or decrease the number of days that capacity summaries will be kept, enter a value for Keep summary measurements for ___ days. Historical data is displayed in capacity graphs for as long as summaries exist. The default is 365 days.

Note Whenever you want to return settings to the factory settings, click the **Restore Defaults** button.

6. Click the **Apply** button to implement your changes and continue working in the Configuration window, or click **OK** to apply your changes and close the window.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0182
Fls:
Doc: 3701

Managed directories

Managed directories are directories whose size you want to monitor. When directories are managed, you can view, report, and set thresholds on their size. Directory size in capacity view panels is the sum of the sizes of all files in the directory, excluding subdirectories and their files. To get the size of a directory including its subdirectories and their files, use the Command Line User Interface (CLUI).

You can select directories to manage once Storage Builder has collected file data. Until then, Storage Area Manager's Directories folders and tabs are empty. A Directories folder contains managed directories, not all directories.

Note To view a list of all directories, managed and unmanaged, on a selected host or volume, click the File/Directory detailed list button in the host Capacity tab or the volume Properties tab.

You can view managed directories for a host, a volume, or the whole domain. Figure 4 shows the contents of a managed directories folder for a selected host:

ECT
2855
CPI - AC

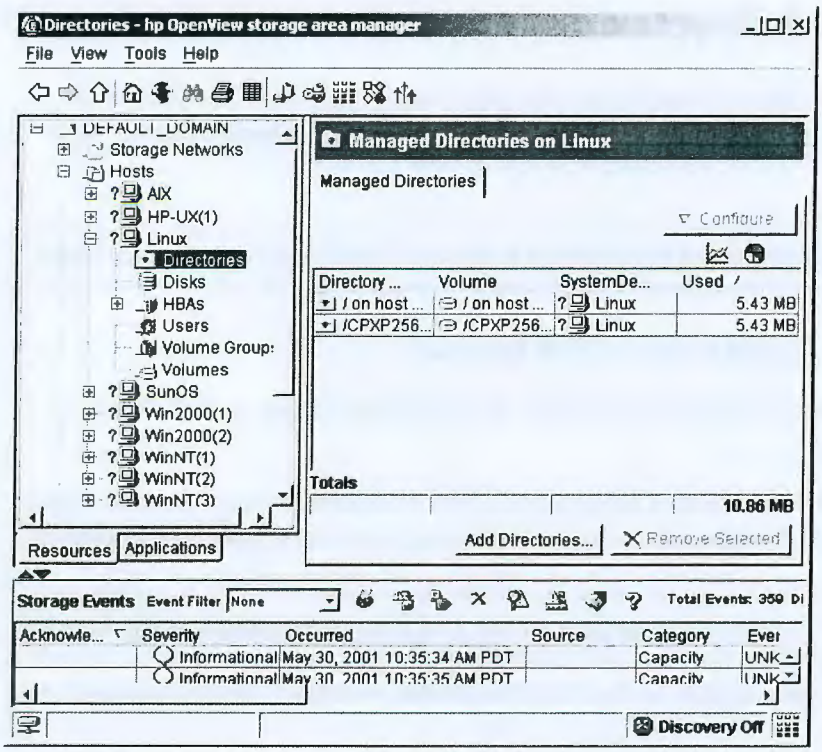


Figure 4 Directories view panel

Click the graph button in managed directory view panels to view directory sizes in the past and predictable future. Click the pie chart button to compare directory sizes. Double-click in a list of managed directories to view the properties of the selected directory, including how much of the volume the directory occupies.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0173
Fls:
Doc: 3701

Adding managed directories

Use this procedure to select directories whose size you want to monitor. The procedure displays a hierarchical list of all directories and subdirectories on a selected host or NAS device.

Note Volume and file data must be collected before you can complete this procedure.

1. In the Resources tree, expand **Hosts** or **NAS Devices**.
2. Expand the specific host or NAS device where the directories exist, and click the **Directories** subfolder.
3. Click the **Add Directories** button at the bottom of the Managed Directories view panel. The Add Directories window displays a tree of volumes, directories, and subdirectories.

Note If no volumes or directories appear in the Add Directories window, make sure that volume and file data was successfully collected. See the online Help topic "When data is unavailable in the Add Directories window" for troubleshooting steps.

4. In the Add Directories window, select one or more directories to be managed. (Use the Control or Shift key to select multiple directories.)
5. Click **OK** to add the selected directories and close the Add Directories window, or click **Apply** to add the selected directories and leave the window open and make more selections.

FCT 2853 fls CPL-AC

Removing managed directories

Use this procedure to discontinue monitoring selected managed directories. The removed directories will no longer appear in the host or NAS device's directories view panels. Removing a managed directory has no effect on the existence of the directory.

1. In the Resources tree, expand **Hosts** or **NAS Devices**.
2. Expand the specific host or NAS device where the directories exist and click the **Directories** subfolder.
3. Select one or more directories in the Managed Directories view panel. (Use the Control or Shift key to select multiple directories.)
4. Click the **Remove Selected** button to remove the selected directories from the list. Any capacity thresholds on the removed directories will also be removed.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0174
Fls:
Doc: 3701

Capacity thresholds

Storage Builder causes Storage Area Manager events when storage usage exceeds or falls below specified limits, called thresholds. You can set thresholds on hosts, volumes, volume groups, managed directories, and users. You can make thresholds global for the domain, common to an organization, or specific to a single resource. You can even set thresholds on future usage. Capacity information is evaluated for threshold violations when it is collected.

Note Thresholds apply in parallel, so multiple threshold events can occur on the same resource.

Threshold events identify the resource, the measured or predicted capacity, and the capacity threshold; for example, "Volume /home on host maine.finance.hp.com usage is 90% which exceeds threshold of 80%." They are reported with whatever severity level you select, and, like other events, can trigger other actions, including e-mail messages, log entries, or commands.

Default capacity thresholds cause informational events when used space exceeds 95% on all hosts, NAS devices, volume groups, and volumes in the domain. Thresholds on predicted capacity are off by default.

Note Volume data must be collected before you can set thresholds on volumes and volume groups. Volume and file data must be collected to set thresholds on directories and users.

ECT 2851 Irene

Setting domain thresholds

Use this procedure to set global consumption alerts on all hosts, NAS devices, volumes, volume groups, managed directories, or users in the domain. The procedure displays a list of the current domain-level thresholds and a window for editing a selected threshold or adding a new one. The new settings take effect at the next collection of capacity data.

1. Select **Configure** from the **Tools** menu.
2. Select **Capacity** under **Thresholds & Alerts** in the Configuration tree. The view panel lists the current thresholds.
3. Click the **Domain** tab if not already selected.

Note To filter the list of thresholds, select a type from the Resource Type drop-down list.

4. To change an existing threshold, including a default threshold, select the threshold(s) and click the **Edit** button. Go to "Entering threshold properties" on page 79 to finish setting the threshold.
5. To add a new threshold, click the **New** button and select a resource type from the drop-down list. See "Entering threshold properties" on page 79 to finish setting the threshold.

Setting organization thresholds

Use this procedure to set consumption alerts on the resources that belong to an organization. The procedure displays a list of the organization's existing thresholds and a window for editing a selected threshold or adding a new one. New and edited thresholds take effect at the next collection of capacity data.

1. Select **Organizations** in the Resources tree.
2. Click the **Capacity** tab in the Organizations view panel.
3. Select one or more organizations from the list in the view panel.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0175
Fls: 77
Doc:
3701

4. Click the **Configure** button and select **Thresholds** from the drop-down menu. The Configuration window lists the existing thresholds of the top selected organization.

Note To filter the list of thresholds, select a type from the Resource Type drop-down list.

5. To modify an existing threshold, select the threshold and click the **Edit** button. Go to "Entering threshold properties" on page 79 to finish setting the threshold.
6. To create a threshold, click the **New** button and select a resource type (host, NAS device, volume, volume group, user, or managed directory) from the drop-down list. See "Entering threshold properties" on page 79 to finish setting the threshold.

Setting thresholds on specific resources

Use this procedure to set consumption alerts on capacity-sensitive hosts, NAS devices, volumes, volume groups, managed directories, or users. The procedure displays a list of the resource's existing thresholds and a window for editing a selected threshold or adding a new one. New and edited thresholds take effect at the next collection of capacity data.

1. Select or expand nodes in the Resources tree as needed to select the collective resource:
   - To set a host threshold, select **Hosts**.
   - To set a NAS device threshold, select **NAS Devices**.
   - To set a volume threshold, expand **Hosts** or **NAS Devices**, expand a particular host or NAS device, and select **Volumes**.
   - To set a volume group threshold, expand **Hosts**, expand a particular host, and select **Volume Groups**.
   - To set a managed directory threshold, expand **Hosts** or **NAS Devices**, expand a particular host or NAS device, and select **Directories**.
   - To set a user threshold, expand **Hosts** or **NAS Devices**, expand a particular host or NAS device, and select **Users**.

2.849

2. Click the **Capacity** tab in the view panel.
3. Select one or more resources from the list in the view panel.
4. Click the **Configure** button and select **Thresholds** from the drop-down menu. The Configuration window lists the existing thresholds of the top selected resource.
5. To modify an existing threshold, select the threshold and click the **Edit** button. Go to "Entering threshold properties" on page 79 to finish setting the threshold.
6. To create a threshold, click the **New** button. See "Entering threshold properties" on page 79 to finish setting the threshold

Entering threshold properties

1. Enter or change the threshold name in the Name box of the Edit Threshold window. You can use letters, numbers, special characters, and spaces. You cannot use more than 64 characters or create duplicate names.

Note If at any time you want to reset threshold settings to the factory defaults, click the **Restore Defaults** button.

2. In the Limit box, enter or change the minimum or maximum amount of used space that will cause a threshold event. (**Direction**, the next labeled box in the window, determines whether the limit is a minimum or maximum.) For user and directory limits, select the unit of measure in the adjacent box. All other limits are percentages (space used over total space). The default limit is 95%.
3. Select **Increasing** in the Direction box to cause a threshold event when used space exceeds the limit value, or select **Decreasing** to cause a threshold event when used space falls below the limit value. The default direction is Increasing.
4. Select the severity level of the threshold event in the Severity drop-down list. The default level is Informational.
5. To set or edit a threshold on future consumption, click the **Trending** tab. Then:

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0176
Fls:
Doc:

- Click **Enable Threshold Trending** to toggle the threshold for future capacity on and off. A check in this box activates the other text boxes in this tab.
- If threshold trending is enabled, select the Projection period, the number of months (1 to 12) into the future that Storage Builder will check for threshold violations. An event will occur if predicted consumption passes the threshold limit any time in the projection period.
- If threshold trending is enabled, select the needed confidence that a threshold violation will be detected. Drag the slider toward More Alerts to increase the confidence up to 95% and toward Fewer Alerts to decrease the confidence down to 5%. Greater confidence allows greater ranges of possible values and therefore increases the likelihood of threshold events. For example, if 95% confidence tests all predicted values within 100 bytes of the threshold limit, then 5% confidence would test predicted values within only 10 bytes of the threshold limit.

6. Click **OK** to close the Edit Threshold window.
7. Click **Apply** to save the settings and continue working in the Configuration window, or click **OK** to save the settings and close the window.

2.847

Deleting capacity thresholds

Use this procedure to remove consumption alerts on hosts, NAS devices, volumes, volume groups, managed directories, or users. The procedure displays a list of the current thresholds at three levels: on individual resources, for an organization, and over the domain. You can select and delete any threshold in the list, including a default threshold.

1. Select **Configure** from the **Tools** menu.
2. Select **Capacity** under **Thresholds & Alerts** in the Configuration tree. The view panel lists the current thresholds.
3. Click the tab that describes the scope of the threshold you want to edit:
   - Click **Domain** to edit a threshold on all like resources in the domain.
   - Click **Organization** to edit a threshold on like resources in an organization.
   - Click **Resource** to edit a threshold on a specific resource.
4. Select the threshold(s) that you want to remove.
5. Click the **Delete** button.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0177
Fls:
Doc: 3701

Capacity reports

Capacity reports help you track the size of certain files and directories in the storage domain. If file data is being collected, you can produce the following reports:

- Stale files have not been opened in a specified number of days. You can get a list of the stale files on a selected host, NAS device, or volume, or you can get the total number and size of all stale files on all the hosts and NAS devices in the domain.
- Junk files can be identified by specific characters, such as .tmp, in their names. You can get a list of the junk files on a selected host, NAS device, or volume, or you can get the total number and size of all junk files on all the hosts and NAS devices in the domain.
- Largest files is a list of the largest files on a selected host, NAS device, or volume. The list includes each file's location, owner, size, file mode, time created, and last time opened or modified.
- Largest directories lists the file contents of the largest directories on a selected host, NAS device, or volume. Contents include each file's location, owner, size, mode, time created, and last time opened or modified.
- Files/directories detailed list is a list of all files and directories on a selected host, NAS device, or volume. The report includes each file's size, owner, file mode, time created, and last time opened or modified. This report is written to a user-specified file and not displayed.

Capacity reports can be printed and exported using Storage Area Manager buttons.

Note File data collection provides the data for file reports.

You define stale files, junk files, and the largest files and directories. You also choose CSV or XML format for the detailed list of files and directories.

2.845

Setting the file format of detailed file/directory lists

Use this procedure to specify the export format for detailed file/directory reports. This is the only report that lists the contents of directories that are not managed and the only report that is automatically exported and not displayed in the report window. The procedure displays the Configuration window with the current export option.

1. Select **Configure** from the **Tools** menu.
2. Select **File-Detail** under **Reports** in the Configuration tree.
3. Select **CSV** or **XML** format from the Export As drop-down list. Storage Builder will save the file list in this format whenever you click the Export button in a report window. The default is CSV.

Note If you want to reassert the factory report settings, click the **Restore Defaults** button.

4. Click **Apply** to save your settings and continue working in the Configuration window, or click **OK** to save your settings and close the window.

Defining file reports

Use this procedure to set up reports of junk files, stale files, and the largest files or directories in managed directories. The procedure displays the Configuration window with the current report specifications. You can change the existing specifications and add new filters.

1. Select **Configure** from the **Tools** menu.
2. Select the report type—**Junk File**, **Largest N-Directories**, **Largest N-Files**, or **Stale Files**—under **Reports** in the Configuration tree. The view panel displays the current report specifications.
3. Select **HTML**, **CSV**, or **XML** in the Export As drop-down list. Storage Builder will save report data in this format whenever you click the Export button in a report window. The default is HTML.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0178
Fls:
Doc: 3701

Note Whenever you want to restore the factory report settings, click the **Restore Defaults** button.

4. In the Sort By boxes, first select the value and then the order that the files will be sorted by in the report. For the value, you can select the file path, type, size, mode, owner, time created, last time modified, or last time accessed. For the order, select **Descending** (higher-to-lower alphabetical or numerical order) or **Ascending** (lower-to-higher alphabetical or numerical order). The default is to sort files by size in descending order, that is, the largest files at the top of the report.
5. In the box Limit Records Per Volume To, select the number of files to include from the top of the selected order. If the files are in ascending order, the report will list the files with lowest values. If the files are in descending order, the report will list the files with the highest values. You can select from 100 to 1000 per volume. The default is 100.
6. If you are defining the stale files report, enter a number in the Days since last access box. This is the number of days that must pass after a file is last accessed before it can be considered stale.
7. To modify an existing filter, click in the rules' cells and select or enter new values.
   - Click **Inclusive** in the rule's Operation cell to view the selectable options **Inclusive** and **Exclusive**. The default is Inclusive.
   - Click in the rule's Pattern cell to enter text in the cell. Patterns are case sensitive and can include global replacement characters (asterisks) at the beginning or end of the character string. Files with the specified character patterns in their names will be included or excluded from the report as specified. The default patterns for junk files are *tmp* and *temp*. For largest files and directories, the default pattern is *. There is no default filter on stale files.
8. To add a rule, click the **Add** button and modify the contents of the Operation and Pattern cells in the new row.
9. To remove a rule, select the rule and click the **Remove** button, or remove all rules by clicking the **Remove All** button.

E C T
2843
Irene
CPI - AC

10. To move a rule up or down in the execution sequence, click the **Up** or **Down** button. Rules are executed in numerical order.
11. Click **Apply** to save your settings and continue working in the Configuration window, or click **OK** to save your settings and close the window.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0179
3701
Doc:

ECT
2842
fls
001-AC

4 STORAGE NODE MANAGER

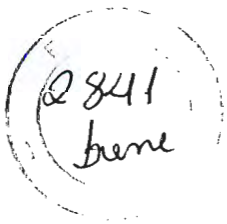
hp OpenView storage node manager features

Configuring device-specific application links

Starting device-specific application links

Viewing device status summary

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0180
Fls: 87
Doc: 3701



hp OpenView storage node manager features

Storage Node Manager is a device status monitoring tool for your storage network. You must install and license Storage Node Manager in order to use these features. Among other features, Storage Node Manager provides:

- Application linking. You can link device-specific applications to Storage Area Manager and then start them from the user interface. An application may be linked to a specific device or device model. Many default device-specific application links are provided with Storage Node Manager.
- Device status monitoring. Storage Node Manager monitors and graphically displays the status of each discovered device in your storage network. Device status is displayed wherever the device is referenced in the user interface, including the Resources tree, device map, and event panel.

  Based on its status inquiries of the storage network, Storage Area Manager generates and displays status-related events as they occur in your storage network.

2840
June

Configuring device-specific application links

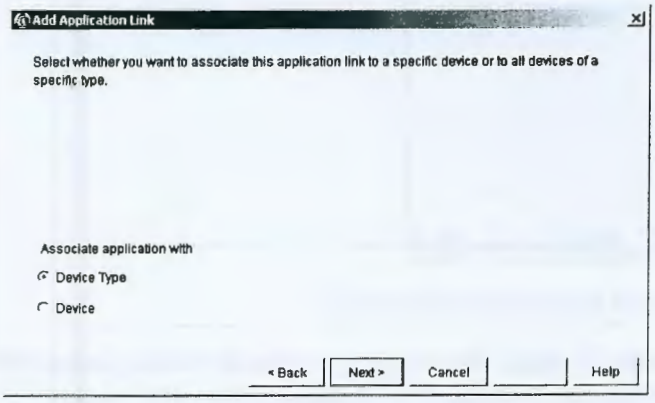
Storage Node Manager's application link feature enables you to start another application from a specific device or device model within Storage Area Manager's user interface. The Add Application Link wizard guides you through the steps necessary for linking the application.

Storage Area Manager provides default application links for many of the devices it supports. These defaults are dependent on each device's management application being installed in its default location.

You can add an application link to a specific device or device model. For example, you may want to link a device-management application to a specific hp StorageWorks switch or to all switches of that model in your storage network

Adding an application link to a device

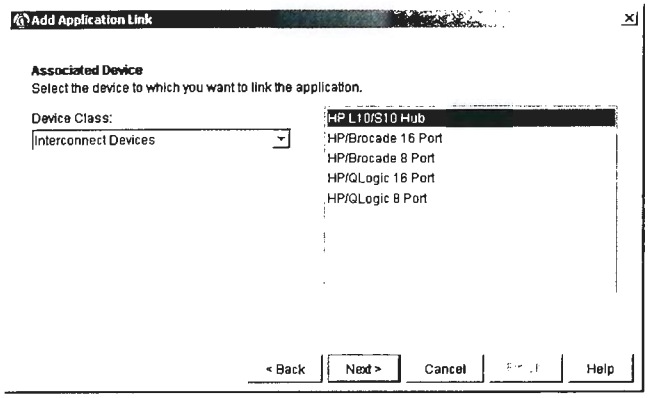
1. From the **Tools** menu, select **Storage Node Manager**, then select **Add Application Link**. The Add Application Link wizard appears.
2. Click the **Next** button to continue. The next wizard panel determines if this application link applies to a specific device or device model.



RQS Nº 03/2005 - CN
CPMI - CORREIOS
0181
Fls:
Doc:
3701

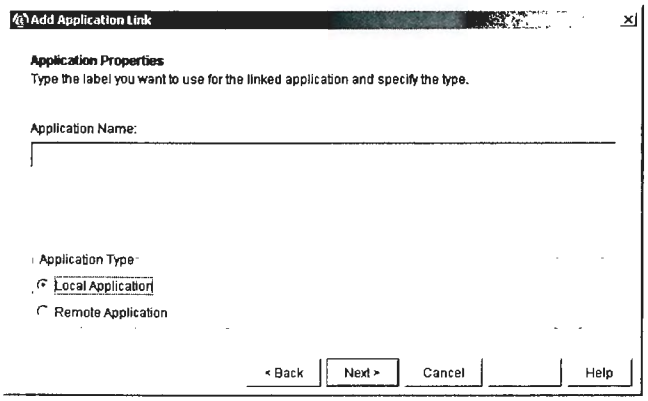
2.839 June

3. Select the **Device** radio button, and click the **Next** button. The wizard's Associated Device panel appears.



4. Select the type of device (interconnect, storage, NAS, bridge, or host) in the Device Class box that represents the device to which you want to link the application.

5. Select the specific device to which you want to link the application in the list box, and click the **Next** button to continue the wizard. The wizard's Application Properties panel appears.

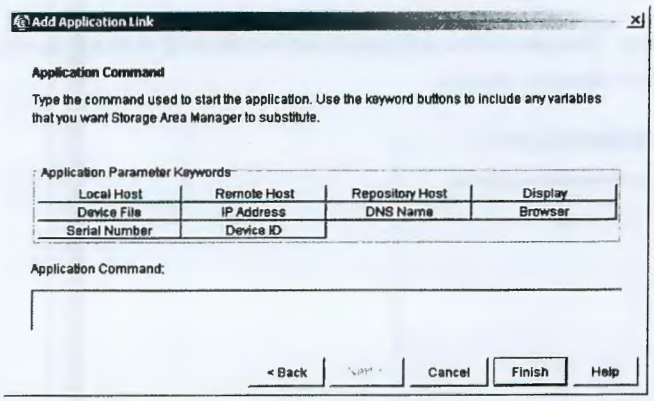


6. Enter the application's name in the Application Name box.

7. Select the **Local Application** radio button if the application you are linking is installed on the host from which you are running Storage Area Manager; otherwise, select the **Remote Application** radio button.

2838

8. Click the **Next** button to continue. The wizard's Application Command panel appears.
9. Enter the command to start the application you are linking in the Application Command box, and click the **Finish** button to add the application link.



You can use the keyword buttons that appear in this panel for variables that you want Storage Area Manager to substitute. See table 1 for a description of each keyword.

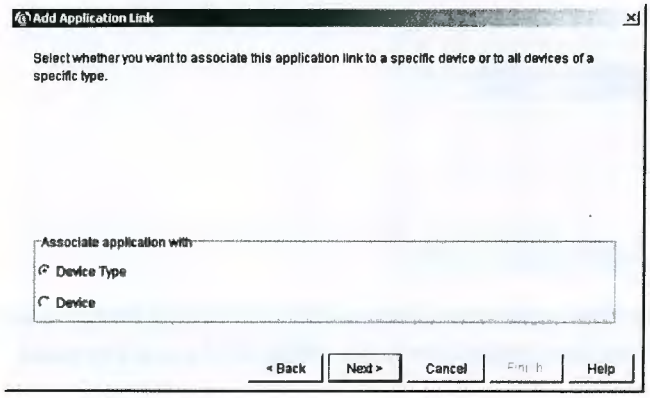
Table 1 Device-specific application link keywords

Keyword	Description
Local Host	The system where the management client is running
Remote Host	Provides a list of available hosts
Repository Host	The management server
Display	Sends display to the management client
Device File	Management path
IP Address	IP address of the selected device
Browser	Launches a web browser **Note** If used, must be the first keyword in the command and must be followed by **http://**
Serial Number	Serial number of the selected device
Device ID	Unique ID of the selected device

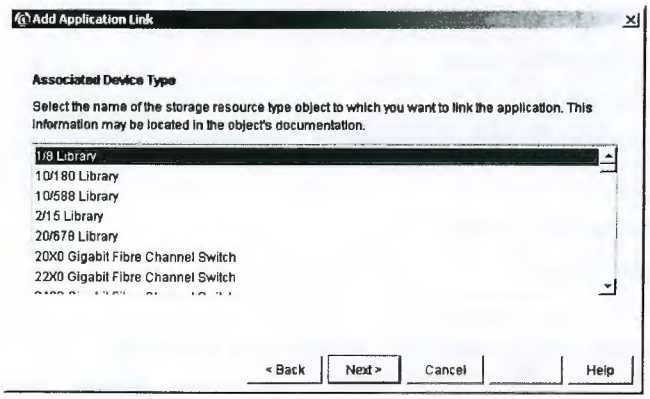
RQS Nº 03/2005 - CN
CPMI - CORREIOS
0182
Fls:
Doc: 3701

Adding an application link to a device model

1. From the **Tools** menu, select **Storage Node Manager**, then select **Add Application Link**. The Add Application Link wizard appears.
2. Click the **Next** button to continue. The next wizard panel determines if this application link applies to a specific device or device model.

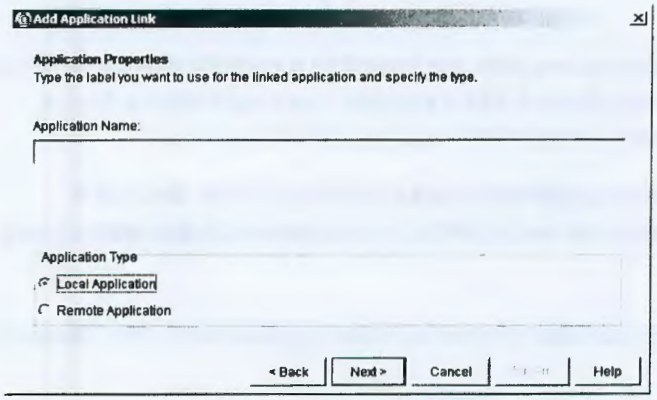


3. Select the **Device Type** radio button, and click the **Next** button. The wizard's Associated Device Type panel appears.

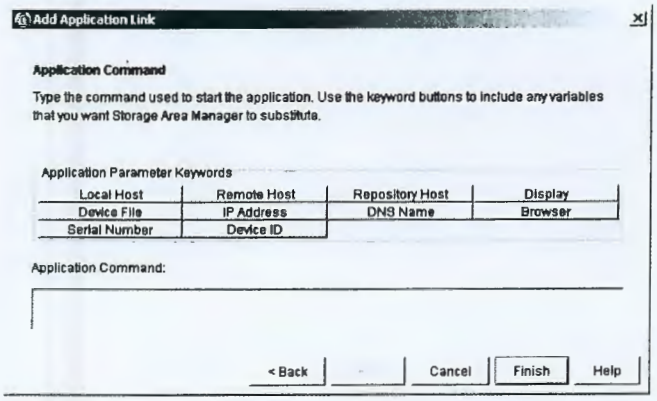


ECT 2836 fls

4. Select the device model to which you want to link the application in the list box, and click the **Next** button to continue the wizard. The wizard's Application Properties panel appears.



5. Enter the application's name in the Application Name box.
6. Select the **Local Application** radio button if the application you are linking is installed on the host from which you are running Storage Area Manager; otherwise, select the **Remote Application** radio button.
7. Click the **Next** button to continue. The wizard's Application Command panel appears.



8. Enter the command to start the application you are linking in the Application Command box, and click the **Finish** button to add the application link.

   You can use the keyword buttons that appear in this panel for variables that you want Storage Area Manager to substitute. See table 1 for a description of each keyword.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0183
Fls:
3701
Doc:

Starting device-specific application links

You can start other management applications that are linked to a specific device or device model if the application was previously linked. For example, you could start a device management application to view more detailed information for that device.

Storage Area Manager provides default application links for many of the devices it supports. These defaults are dependent on each device's management application being installed in its default location.

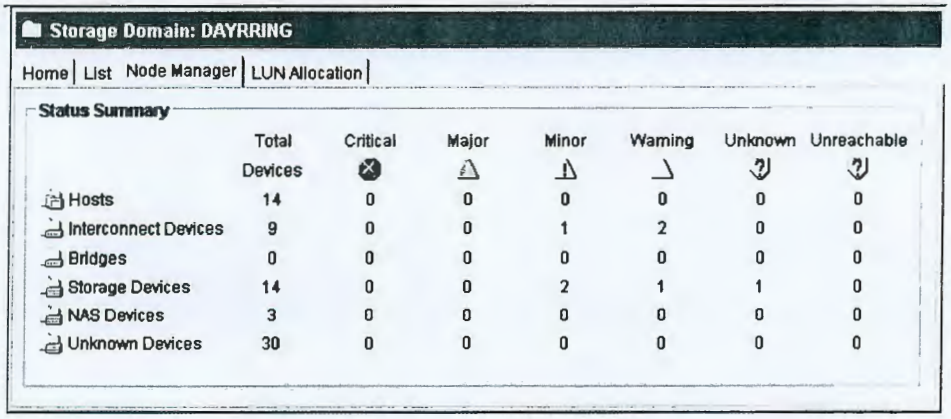
1. Right-click the device for which you want to start a linked application in the Resources tree or device map
2. Select the menu command that represents the application from the device's shortcut menu.
3. If this link represents a remote application, select the host on which the application is installed from the Remote Host window, and click the **OK** button

ECT
2834
Fls.
CPI - AC

Viewing device status summary

You can view a status summary of all discovered devices from one view panel. Storage Node Manager summarizes how many devices are currently in each level of status by device type.

From the **Tools** menu, select **Storage Node Manager**, then select **Storage Domain Status Summary**.



	Total Devices	Critical	Major	Minor	Warning	Unknown	Unreachable
Hosts	14	0	0	0	0	0	0
Interconnect Devices	9	0	0	1	2	0	0
Bridges	0	0	0	0	0	0	0
Storage Devices	14	0	0	2	1	1	0
NAS Devices	3	0	0	0	0	0	0
Unknown Devices	30	0	0	0	0	0	0

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0184
Fls:
Doc: 3701

2833

5 STORAGE OPTIMIZER

hp OpenView storage optimizer features

Performance metrics

Performance data collection

Performance data archiving

Performance baselines and automatic thresholds

Performance charts

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0185
Fls:
3701
Doc:

2.832
June

hp OpenView storage optimizer features

Storage Optimizer monitors and reports the performance of storage network resources. Performance metrics vary by resource, but typical metrics are read and write rates, byte transfer rates, average queue depths, various errors, invalid CRCs and transmission words, link failures, signal losses, received and transmitted bytes and frames, read and write operations, read and write cache hits, and blocks requested. Storage Optimizer can display any metric that a resource supports. You must install and license Storage Optimizer to use its features.

Storage Optimizer adds the following features to Storage Area Manager:

- Performance views of host disks, volumes, HBAs, interconnect devices, storage devices, LUNs, and controllers.
- The ability to view devices in the order of their performance on a common metric. This allows you to compare performance across like devices and to easily identify the top (or bottom) performers. You can limit long lists to the first 5, 10, 15, and so on, up to 100 or all devices.
- Line charts of the performance data that was collected for individual devices over selectable periods of time. You can define your own charts to supplement the charts that Storage Optimizer provides.
- Performance trends. Line charts can show you where performance is likely to be in the near and distant future based on current trends. Using sophisticated statistical models, Storage Optimizer identifies trends that can account for such influences as seasonal variation. You can turn this feature on or off, and you can select from the simplest to the most sensitive predictive models.
- Baselining and automatic thresholds. Using the most sophisticated statistical analysis, Storage Optimizer can establish an extremely accurate baseline of expected performance. At your option, Storage Optimizer will send a threshold event whenever actual performance deviates significantly from the baseline.

2.831

- Data export. The button saves the contents of performance charts in a comma-delimited (CSV) file.
- Secure access to administrator functions. Only administrators can enable/disable the collecting, baselining, and automatic thresholding of performance data, or schedule the summarizing and archiving of performance data.
- Command Line User Interface (CLUI). Run-line commands expedite the viewing and configuring of Storage Optimizer information.
- Support for OpenView Operations and OpenView Reporter queries of the performance database.

IRQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 0186
3701
Doc: 99

Performance metrics

Storage Optimizer collects performance information on the following resources and their components:

- Host disks, volumes, HBAs, and HBA ports
- Interconnect devices and their ports
- Storage devices and their LUNs, disks, and controllers

The specific metrics that Optimizer collects depend on the resource. Storage Optimizer is designed to display any performance metric that a resource supports. You can view the metrics collected for individual resources by viewing performance data collection in the Configuration window.

Performance data collection is off until you enable collection for selected resources. When collection is enabled, the default is to collect all metrics for hosts and common metrics for storage and interconnect devices.

All metrics

All metrics includes the custom and common metrics that a resource supports. Individual resources provide various custom metrics depending on the model and the manufacturer. Storage Optimizer displays custom (and common) metrics in charts when you select a specific device in the Resources tree.

All metrics is the default choice for performance data collection on hosts and HBAs. There are currently two kinds of host metrics, one provided by the OpenView Operations Performance Agent (OVPA) and the other by OpenView VantagePoint (VP).

OVPA on any host and VP on UNIX hosts support the following metrics for host disks:

- Physical read rate (display default)
- Physical write rate

OVPA and VP on HP-UX hosts support the following metrics for host disks and volumes:

- Physical read rate (display default)
- Logical read and write rates
- Physical write rate

VP on Windows hosts provides the following metrics for host disks and volumes:

- Bytes transferred per second (display default)
- Average queue depth length

For HBAs and HBA ports, Storage Optimizer collects all of the performance metrics in the SNIA library. If an HBA has no SNIA driver or does not support SNIA's performance metrics, there is no Performance tab in the view panel. If the HBA supports any SNIA performance metrics, the Performance tab will display them.

Common metrics

Storage Optimizer attempts to collect a common set of metrics for all storage devices and all interconnect devices. Common metrics allow you to compare the performance of like resources. In fact, Storage Optimizer lists resources in order of their performance on a common metric when you select the collective resource in the Resources tree.

The following common metrics are the default choice when data collection is enabled for a storage or interconnect device. The default metric shown in resource lists is in bold.

Common metrics for interconnect devices:

- **Total errors** (display default)
- Invalid CRCs
- Invalid transmission words
- Link failures
- Primitive sequence protocol errors
- Received bytes and frames
- Signal losses

- Synchronization losses
- Transmitted bytes and frames

Common metrics for ports on interconnect devices:

- **Total errors** (display default)
- CRC errors
- Invalid CRCs
- Invalid transmission words
- Link failures
- Primitive sequence protocol errors
- Received frames
- Signal losses
- Synchronization losses
- Transmitted frames

Common metrics for storage devices:

- **Total operations** (display default)
- Percentage of reads and writes from cache
- Read and write cache hits
- Read and write operations

Common metrics for LUNs:

- **Total operations** (display default)
- Percentage of reads and writes from cache
- Read and write cache hits
- Read and write operations

2.827

Performance data collection

Storage Optimizer collects performance data on selected resources. You select the resource and configure Storage Optimizer to collect all or only the common metrics that the resource supports. Common metrics is the default choice for all but hosts. Metrics can be collected on host disks and volumes, HBAs, HBA ports, storage devices, LUNs, controllers, switches, and switch ports.

Collection schedule

Storage Optimizer collects performance metrics on selected resources and their components every 15 minutes. It holds the data in its memory until the top of the hour, when it summarizes the quarter-hour data into a single hourly value. If the metric is a rate, such as bytes transferred per second, the hourly value is the average of the collected data. If the metric is a count, such as the number of bytes transmitted, the hourly value is the sum of the collected data. The hourly values are stored in Storage Area Manager's database and viewed in performance lists and charts.

Enabling/disabling metrics collection

Use this procedure to start or stop the collection of performance metrics for a selected resource. You can enable collection for all metrics or for only the common metrics that the resource supports. The change will take effect at the next collection cycle.

1. Select **Configure** from the **Tools** menu.
2. Select **Performance Data Collection** from the Configuration tree. The view panel displays a list of the resources that provide performance metrics and the status of collection and baselining for each.

Note If the list is long, you can limit it to a single type of resource. Select **Hosts**, **Interconnect Devices**, or **Storage Devices** from the Device Type list.

RQ3 N° 03/2005 - CN
CPMI - CORREIOS
0188
Fls:
Doc: 3701

3. Select the host or device that needs a collection change.
4. Click the **Edit** button. The Collection/Baselining window opens.
5. Click the **Collection** tab if it is not already selected.
6. Click the **Collect Metrics** check box to toggle collection on or off for the selected resource. When the box is checked, collection is enabled and the window shows the list of metrics being collected. No collection is the default.
7. If collection is enabled (step 6), select the **Collect Common Metrics** or **Collect All Metrics** button to set the scope of metrics collected. The default is to collect common metrics for all resources but hosts. The list in the bottom half of the window shows which metrics are collected at the selected scope. Any common metrics that the device does not support are not listed.
8. Click **OK** to apply your selections and close the Collection/Baselining window.
9. Select another resource and repeat steps 4 through 8, or click **OK** to apply the changes and close the Configuration window.

2.825

Performance data archiving

On a schedule you choose, hourly values are summarized into a daily archive. The default archive schedule is 7 days after the hourly data is created, but you can choose from 1 to the number of days that archives are retained. Reducing 24 values to one for hundreds of collected metrics obviously saves space in the database. Yet other management objectives may require keeping hourly data as long as possible. To establish the hours of peak demand on a volume or switch port, for example, you may need hourly metrics for 2 weeks or more. To get the most precise prediction of LUN operations or any other metric, for another example, you should use a smoothing analysis model, which requires hourly data, the more the better.

Archive retention

You also determine how long performance data is kept in the database. The default retention period is 31 days, but you can select up to 365 days. Again, a balance must be struck between database economy and other management objectives. The more historical data that is available for trend analysis, for example, the more accurate the predictions will be.

Scheduling performance archives

Use this procedure to set the schedule for archiving and summarizing performance data.

1. Select **Configure** from the **Tools** menu.
2. Select **Performance Archiving** below **Scheduling** in the Configuration tree.

Note If at any time you want to restore the schedules to the factory defaults, click the **Restore Defaults** button.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 0189
Doc: 3701

3. In the upper text box, enter the number of days that performance data will be saved. You can enter the value or click the up and down arrows to increase or decrease the value one day at a time. Click the **Restore Default Charts** button.

4. In the lower text box, enter the number of days that collected data will be kept before it is summarized. Valid values are 1 to the number of days performance data is kept (see step 3). The default is 7 days.

5. Click **OK** to apply the values and close the Configuration window.

ECT
2.823
Bruna

Performance baselines and automatic thresholds

Storage Optimizer can let you know when selected resources are performing abnormally. Based on a statistical analysis of collected metrics, Storage Optimizer can construct an extremely accurate baseline representing normal performance. If the next collected metric deviates significantly from the baseline value, Storage Optimizer automatically generates a threshold event warning.

Baselining requires hourly data points for twice the selected season length. The default season length is one day, so by default Storage Optimizer requires two days' worth of hourly data to determine the baseline. The more hourly data available, the more reliable the prediction will be.

Note When count data is displayed as rates, the baseline is recalculated for the period displayed in the chart and baseline values do not appear until the 49th hour of the data displayed.

Baseline parameters

Storage Optimizer uses the most sensitive analysis model, called triple exponential smoothing, to calculate the baseline. This model is sensitive to three different variables in the data:

- Baseline sensitivity emphasizes more recent data in calculating the baseline.
- Trend sensitivity emphasizes the upward or downward tendency of the data in calculating the baseline.
- Seasonality sensitivity emphasizes the periodic tendency of the data, that is, the tendency to repeat a pattern of variance over specific periods of time. The length of the period (season) is selectable.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0190
Fls:
3701
Doc:

You can increase or decrease these sensitivities according to the importance of the variables for the device being monitored. In addition, you can set the threshold sensitivity, which determines how much deviation from the baseline is sufficient to cause a threshold warning.

Baseline limitation

The number of metrics that can be baselined depends on the processing resources of the management server. For that reason, Storage Optimizer limits baselining to a portion of the metrics that can be collected on a device and keeps a running balance of the total number of baselines that can be set. When baselining is enabled on a device, Storage Optimizer calculates how many baselines would be needed if the device supported all the baselinable metrics. Baselinable LUN and port metrics are multiplied by the number of LUNs or ports, respectively, on the device. Storage Optimizer then subtracts the number of potential baselines from the total number of baselines available and displays the balance when you view baseline thresholds.

Enabling/disabling baseline thresholds

Use this procedure to enable or disable performance baselining or threshold events for a selected resource. The result is a list of resources that support performance metrics and the status of baselining and thresholding for each.

1. Select **Configure** from the **Tools** menu.
2. Select **Performance Data Collection** from the Configuration tree. The view panel shows the status of collection and baselining for all resources that support performance metrics.

Note If the list is long, you can limit it to a single type of resource. Select **Hosts**, **Interconnect Devices**, or **Storage Devices** from the Device Type drop-down list.

3. Select the resource that you want to change.
4. Click the **Edit** button.

2.821
fls.
CPI - AC

5. Click the **Baselining/Threshold** tab in the Collection/Baselining window.
6. Click the **Enable Baselining** check box to toggle baselining on or off. When the box is checked, baselining is enabled and the Show Events option and baselining parameters are active. Default baselining is off.
7. If baselining is enabled (step 6), click the **Show Events** check box to toggle threshold events in the event panel on or off.
8. If baselining is enabled (step 6), set the baselining parameters as needed. The default values give a small but significant sensitivity to the respective variables: baseline, trend, seasonality, and threshold. Click the right-facing arrows to increase the sensitivity of one or more variables; click the left-facing arrows to decrease the sensitivity. Increasing the threshold sensitivity decreases the likelihood of threshold events.

   Also select the length of the season, a day or a week, from the Season Length drop-down box.
9. Click **OK** to apply your settings and close the Collection/Baselining window.
10. Choose other resources and turn baselining on or off, or click **OK** to close the Configuration window.

Storage Optimizer

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0191
Fls:
Doc:

Performance charts

Performance charts are line graphs showing the changes in a performance metric (y axis) over time (x axis). The chart in figure 5 shows the number of read operations on a selected LUN between October 4 and October 9, 2002 (the day that the chart was generated), and the number of read operations projected for October 9 to October 13, 2002. The straight line from about October 7 to midday October 8 shows a lapse in the collection of data.

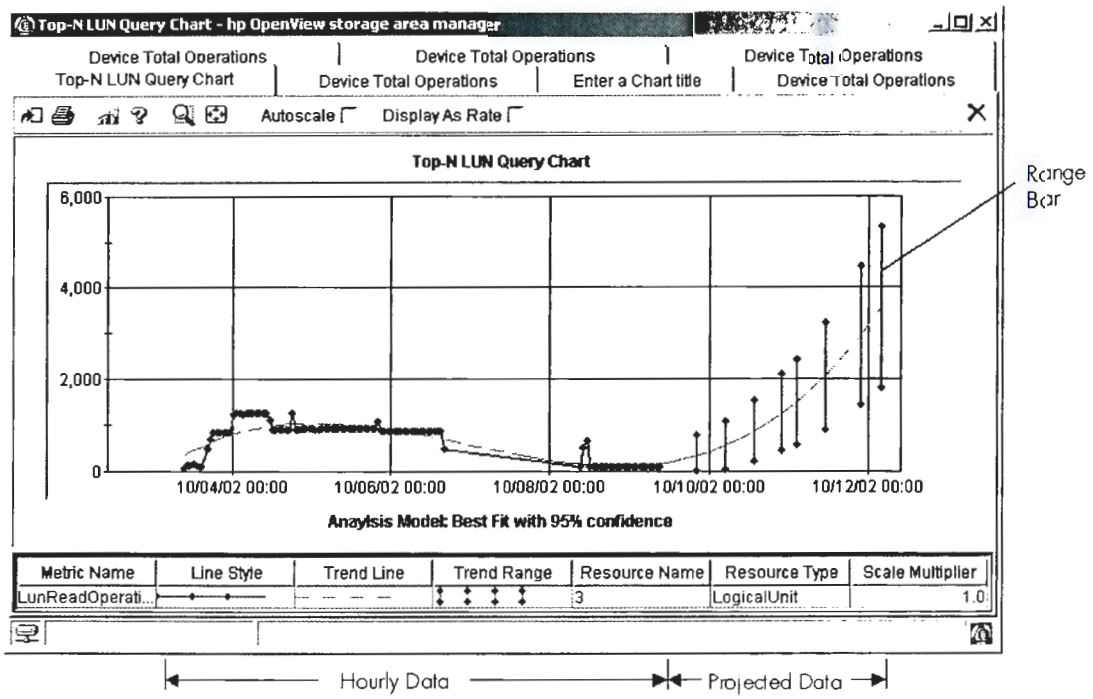


Figure 5 Sample performance chart

ECT 2.819 fls CPI - AC

This chart contains hourly and projected data. Charts can also contain archived data.

- Archived data. Data that is more than 7 days old, by the default archive schedule, is summarized into one data point per day. Rate data is averaged, and count data is added to obtain the daily value. When a chart contains archived data, all data points are presented as daily values.
- Hourly data. Storage Optimizer collects data every 15 minutes, but stores and displays hourly summaries of the collected data. Charts for periods less than the archive schedule contain hourly data and are noticeably denser than charts that contain archived data. Also, for count data, the y values of archived and hourly data points differ because each archived data point is the sum of 24 hourly data points.

Note Displaying count data as rates obscures the difference between archived and hourly data.

- Projected data. When a chart includes trend data, a broken line shadows past data and extends into the future. This line represents a pattern analysis of collected data and the projection of that pattern into the future. Vertical bars along the projected values show the range of possible values based on the required confidence. Greater confidence in the prediction implies greater ranges. The confidence specified for the sample chart is 95%.

  Projections must be interpreted according to the model that is used to make the analysis. The analysis model is indicated at the bottom of the chart. In the example here, the analysis model is best fit. Linear and other nonsmoothing models use archived and hourly data to predict future rate data points. If count data is displayed or if the analysis model is smoothed, only hourly data is used for the prediction.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0192
Fls:
Doc: 3701

Managing performance charts

Use this procedure to delete all custom (user-defined) performance charts or to restore all default (factory-defined) performance charts. The procedure displays a list of the custom and default performance charts that are currently available for interconnect or storage devices.

Note To delete individual charts, use the procedure "Deleting performance charts".

1. Select **Configure** from the **Tools** menu.
2. Select **Performance Charts** in the Configuration tree.
3. To restore any factory-defined charts that have been deleted, click the **Restore Defaults** button.
4. To delete all user-defined charts, select the **Remove User-Defined Charts** button.
5. Click **Apply** to accept changes.
6. Click **OK** to close the Performance Charts window.

Deleting performance charts

Use this procedure to delete a factory-defined or user-defined chart that is not needed in your environment.

Note You can restore default charts at any time.

1. Expand **Storage Devices** or **Interconnect Devices** in the Resources tree, depending on which devices the chart was defined for.
2. Select an individual device in the expanded tree.
3. Click the **Performance** tab.
4. Use the right mouse button to select the chart to be deleted, and select **Delete Chart** from the shortcut menu.

2.817
Irene

Restoring default charts

Use this procedure to undelete factory-defined charts for interconnect or storage devices. Any default charts that were previously deleted will return to the list.

Note An administrator can restore all default charts in one action using the Configuration tool.

1. Expand **Storage Devices** or **Interconnect Devices** in the Resources tree, depending on which devices the default charts describe.
2. Select an individual device in the expanded tree.
3. Click the **Performance** tab.
4. Click the **Restore Default Charts** button.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0193
Fls:
Doc: 3701

2.816
fls

6 STORAGE ALLOCATER

hp OpenView storage allocater features

Groups

Managing assignments

Managing hosts

Managing LUNs

hp OpenView storage allocater interoperability

RQS Nº 03/2005 - CN
CPMI – CORREIOS
0194
Fls:
Doc: 3791

hp OpenView storage allocater features

HP OpenView Storage Allocater controls storage access and provides security by assigning logical units (LUNs) to specific hosts or share groups. Assigned LUNs cannot be accessed by any other hosts. With this application, you can assign, unassign, and reassign storage and related devices from a diverse pool. You must activate and license Storage Allocater to use these features.

Storage Allocater brings the following features to Storage Area Manager:

- *Security groups*. Share groups and associated LUN groups help to streamline storage assignments. Share groups allow hosts to share the same storage devices. Associated LUN groups keep sets of LUNs (for example, stripe sets or mirror sets) together, requiring them to be assigned and unassigned as a unit.
- *Organizational groups*. Host groups and LUN groups allow you to arrange hosts and LUNs into hierarchical groups in the Storage Area Manager user interface.
- *Reports*. Storage Allocater can generate reports that show all LUNs, assigned LUNs, or unassigned LUNs. These reports allow you to quickly view the assignment status of all the LUNs in the current storage domain.
- *System availability*. Storage Allocater provides increased system availability by enabling storage to be assigned, unassigned, and reassigned without reboots.

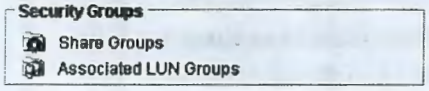
Groups

After activating Storage Allocater you can create security and organizational groups. These groups are optional, but they help you to streamline storage assignments and organize information within the Storage Area Manager user interface

Security groups

Share groups and associated LUN groups are called security groups because their manipulation affects storage access. Unlike organizational groups (page 119), security groups are not hierarchical; security groups cannot be members of other security groups.

When you select Storage Allocater in the Applications tree, the view panel displays the LUN Allocation tab, which contains shortcuts to Storage Allocater's security groups.



Share groups

Share groups allow multiple hosts to share the same storage with read-write access.

Caution When using share groups, you must use an application that preserves data integrity on shared storage. Without this type of application, data corruption may occur.

Share groups operate according to the following rules:

- When you assign or unassign a share group host, all of the storage in the share group is assigned to or unassigned from the host. If all of the storage in a share group cannot be assigned or unassigned, the assignment or unassignment request will fail.
- When you assign or unassign share group storage, it is automatically assigned to or unassigned from each host in the share group. If all of the LUNs in the share group cannot be assigned or unassigned, the assignment or unassignment request will fail.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0195
Fls:
Doc: 370

Associated LUN groups

Associated LUN groups are used for any set of LUNs that needs to be assigned and unassigned as a unit; for example, stripe sets, mirror sets, and sets of LUNs that contain parts of the same database. When a LUN is assigned to an associated LUN group, it cannot be assigned or unassigned as a separate item until it is removed from the associated LUN group. Associated LUN groups use the following rules:

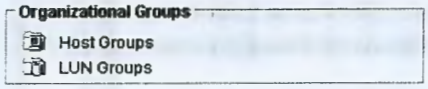
- When you assign an associated LUN group to a host or share group, all of the LUNs in the associated LUN group are assigned to the single host or all of the share group hosts. If all of the LUNs are not successfully assigned, the assignment of the associated LUN group will fail.
- When you unassign an associated LUN group from a host or share group, all of the LUNs in the associated LUN group are unassigned from the affected hosts. If all of the LUNs are not successfully unassigned, the unassignment of the associated LUN group will fail.
- If you add a LUN to an associated LUN group while the associated LUN group is assigned to a host or share group, the newly assigned LUN is automatically assigned to the single host or the hosts in the share group. If the new LUN is not successfully assigned, the assignment of the LUN to the associated LUN group will fail.
- If you unassign a LUN from an associated LUN group that is assigned to a host or share group, the unassigned LUN is automatically unassigned from the affected hosts. If the LUN is not successfully unassigned, the unassignment of the LUN from the associated LUN group will fail.

Tip For detailed rules for using share groups and associated LUN groups, see the "About share groups" and "About associated LUN groups" topics in the Storage Area Manager online help system.

Organizational groups

Host groups and LUN groups are called organizational groups because they are used to organize information in the Storage Area Manager user interface, but manipulation of these groups does not directly affect storage access.

When you select Storage Allocater in the Applications tree, the view panel displays the LUN Allocation tab, which contains shortcuts to Storage Allocater's organizational groups.



Organizational groups allow you to create a hierarchy of groups. When configuring and viewing organizational groups, you may have to expand several group levels in order to select a group. For example, to view the members of the Engineering Servers host group shown here, you would expand the Building A host group.

Tip For detailed rules for using host groups and LUN groups, see the "About host groups" and "About LUN groups" topics in the Storage Area Manager online help system.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0196
Fls:
Doc:

Managing assignments

Assignment types

There are three types of assignments in Storage Allocater.

- When you assign items to host groups and LUN groups, the items become part of an organizational structure that is displayed in the Storage Area Manager user interface.
- When you assign storage to a host or share group, the individual or grouped hosts are granted read-write access to the assigned storage.
- When LUNs are grouped into an associated LUN group, they are bound together and must be assigned and unassigned as a unit.

In general, unassignments work the same way as assignments. When you unassign items from an organizational structure, they are removed from that structure, and when you unassign storage from a host or share group, the storage is no longer available to the affected host(s).

Note For instructions on editing Storage Allocater assignments, see the Storage Area Manager online help system.

Assignment rules

Table 2 lists the assignments that can be made in the Storage Allocater user interface.

Table 2 Storage Allocater assignments

	Assignable items				
	LUN	**LUN group**	**Associated LUN group**	**Host**	**Host group**
Hosts	X		X		
Associated LUN groups	X				
Share groups	X		X	X	
LUN groups	X	X			
Host groups				X	X

To edit a host's assignments, right-click the host in the Resources tree and select **LUN Allocation**. To edit a group, right-click the group in the Applications tree and select **Edit Assignment**.

Note For specific instructions on editing assignments, see the Storage Area Manager online help system.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0197
Fls:
Doc: 3701

Special unassignments

In some cases, usually when a host or share group cannot release LUNs that are in use, a host, LUN, or associated LUN group cannot be unassigned with the **Unassign** command. In these cases, check the involved Windows, Solaris, Linux or AIX hosts and try to solve the issue that prevents the unassignment. For tips on troubleshooting unassignments, see chapter 8. If the item still cannot be unassigned, use the **Special Unassign** command, which requires a reboot of all affected hosts.

The following rules apply to special unassignments:

- The **Special Unassign** command is available when you right-click a host, LUN, or associated LUN group in the Assigned section of the Edit window.
- A special unassignment is not complete until you reboot all the affected hosts. After an affected host is rebooted, a message similar to the following appears in the event panel: `Special unassignment of host <host name> from share group <group name> completed.`
- Before you can assign or re-assign the LUNs that were involved in a special unassignment, you must reboot all the affected hosts.
- Special unassignments are not required on HP-UX hosts, so the **Special Unassign** command is unavailable when you are configuring HP-UX hosts or share groups that contain HP-UX hosts. If a LUN cannot be unassigned from an HP-UX host, follow the instructions on page 206.
- You cannot special unassign hosts from a share group at the same time that LUNs or associated LUN groups are being special unassigned. You must special unassign hosts and storage separately.
- You can use the **Special Unassign** command to unassign the following items:
  - A host from a share group.
  - A LUN from a host, share group, or associated LUN group.
  - An associated LUN group from a host or share group.

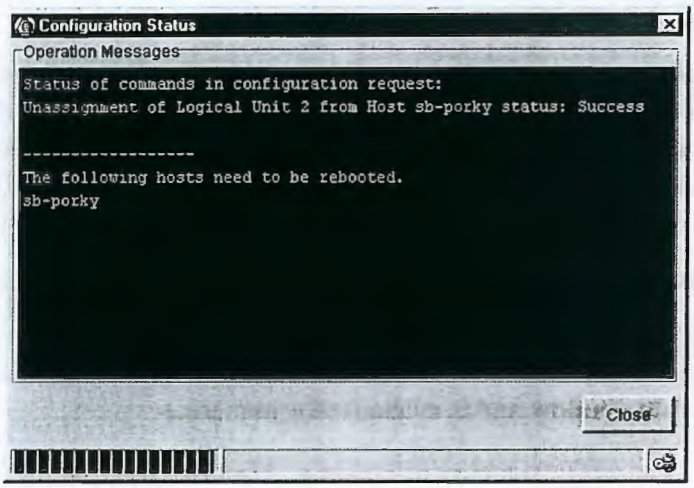
E C T
2.808
fls.
CPI - AC

Using the Special Unassign command

- When you right-click one or more assigned items and select **Special Unassign**, the selected items are dimmed in the list on the right and added in magenta to the Unassign List on the left. A green-and-magenta arrow appears in the Status column beside the moved items in each list, indicating that a special unassignment is pending.
- Until you click the **Apply** button, you can undo a pending special unassignment by selecting an item in the Unassign list and clicking the **Undo** button or by dragging the item from the Unassign List into the Assigned section of the Edit window. Once you apply a special unassign request, you cannot undo the request, and you must reboot the affected hosts.
- When you try to perform a special unassignment, Storage Area Manager first tries a regular unassignment.
  - If the regular unassignment is successful, the item that was unassigned is removed from the Assigned section of the Edit window and is available for immediate assignment elsewhere.
  - If a regular unassignment is not possible, the item remains in the Assigned section of the Edit window, and is listed in magenta text.
- If a host that is involved in a special unassignment is in one or more share groups, the host is listed in magenta text in the Edit Share Group window until it is rebooted.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0198
Fls:
Doc: 3701

- When you click **Apply**, the Configuration Status window opens and reports the status of the requested special unassignment. If hosts need to be rebooted, they are listed in the Configuration Status window and in the event panel. The message in the Configuration Status window is similar to the following:



Note For specific instructions for using the **Special Unassign** command, see the following online help topics: "Special Unassigning Hosts," "Special Unassigning a LUN," and "Special Unassigning Associated LUN Groups."

2.806 June

Assigning LUNs for Windows Clustering

Windows Clustering (Windows 2000)

The following information can be helpful when running Storage Allocater with Windows Clustering:

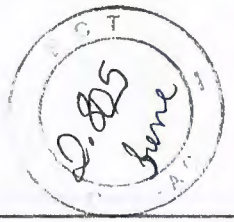
- When a server cluster host is reserving a LUN, the Storage Area Manager user interface may show management paths as down because the reservation of the LUN prevents Storage Allocater from reading the LUN.
- If the quorum disk is not an active resource on a cluster host, the disk may not be displayed in Disk Management.
- Do not unassign a quorum disk from a running cluster's share group. The quorum disk must be accessible to all hosts in the cluster for failover to work.
- For instructions on configuring your HBA drivers for use with clustering, see the documentation that came with your HBA.
- If Windows Clustering is set up before Storage Allocater is activated, use the Storage Allocater Activation wizard to create the server cluster share group.

Setting Up a Server Cluster Share Group

1. Before setting up a server cluster share group, read the Windows 2000 "Server Clusters" online help topics, and pay attention to the required order of attaching, partitioning, and configuring shared disks.
2. Create a share group.
3. Assign the LUNs that will be used by the cluster to the share group.
4. Assign one of the cluster hosts to the share group.

Note For instructions on creating and editing Share Groups, see the "Adding Share Groups" and "Assigning Share Group Members" topics in the Storage Area Manager online help system.

ECT 1.806-0199 CPMI-CORREIOS Fls: 3751 Doc:



5. Follow the steps in the Windows 2000 online help topic "Checklist: Creating a Server Cluster." When using the checklist, note the following guidelines:
   - Partition and format the cluster disks on the host that was assigned to the share group in step 4.
   - All of the shared cluster disks must have the same assigned drive letter on each host in the share group. To accomplish this, assign one host to the share group at a time, configure the drive letters, then unassign the host from the share group and repeat this step for all hosts that will be included in the cluster.
   - When following the procedures in the "Creating a Server Cluster" checklist, only one host at a time should be assigned to the server cluster share group.
6. Install the cluster service on the host in the cluster share group.
7. Add all of the other cluster hosts to the share group.
8. Install the cluster service on all of the other hosts in the cluster share group.
9. Configure Windows Clustering according to the instructions in your Microsoft documentation.

Note You may need to re-apply current service packs after installing Windows Clustering for the first time. See your Microsoft documentation for more information.

Microsoft Cluster Server (Windows NT 4)

The following information is be helpful when running Storage Allocater with Microsoft Cluster Server (MSCS):

- When you repartition a LUN that is on the same virtual bus as the quorum disk, all partitions on the disk may become inaccessible when you commit the changes in Disk Administrator. To access the LUN, reboot the host that did the repartitioning.
- When an MSCS host is reserving a LUN, the Storage Area Manager user interface may show LUNs or management paths as down or offline because the reservation prevents Storage Allocater from reading the LUN.

ECT 2.804 Irene

- If the quorum disk is not an active resource on a cluster host, Cluster Disk (the MSCS disk filter) prevents that host from seeing the disk in Disk Administrator.
- MSCS may not be able to use a disk that is added dynamically to a running host. In some cases, the host must be rebooted for MSCS to begin using the disk. For example, if the quorum disk is unassigned from a host and assigned to the host again, MSCS will not begin using it until you reboot the host.
- For instructions on configuring your HBA drivers for use with MSCS, see the documentation that came with your HBA.
- Storage Allocater LUNs cannot be unassigned from a cluster share group while MSCS is running because the MSCS drivers have an open reference to the LUNs. To unassign these LUNs, use Storage Allocater's **Special Unassign** command. For more information about the **Special Unassign** command, see page 122.
- If MSCS is set up before Storage Allocater is activated, use the Storage Allocater Activation wizard to create the MSCS share group.

Setting Up an MSCS Share Group

1. Create a share group.
2. Assign the LUNs that will be used by the cluster to the share group.
3. Assign one of the cluster hosts to the share group.
4. From the cluster host in the share group, partition and format the cluster storage according to MSCS requirements. See your Microsoft documentation for instructions.
5. Assign the remaining cluster hosts to the share group.

Note For instructions on creating and editing Share Groups, see the "Adding Share Groups" and "Assigning Share Group Members" topics in the Storage Area Manager online help system.

Caution Do not access the shared storage until MSCS is set up.

ROS Nº 03/2005 - CN
CPMI - CORREIOS
0200
Fls:
Doc: 3791

6. For easy identification, configure the drive letters to match on each cluster host.
7. Install MSCS onto all of the share group hosts.
8. Configure MSCS according to the instructions in your Microsoft documentation.

Note You may need to reapply current service packs after installing MSCS for the first time. See your Microsoft documentation for more information.

Assigning LUNs for volume management software

When assigning LUNs for use with volume management software, the following guidelines apply:

- When an assigned LUN is part of a volume set, it cannot be unassigned by Storage Allocater. To unassign a LUN that is in a volume set, remove the LUN from the volume set, and then unassign it from the affected host or share group.
- If storage network LUNs are configured into volume sets before Storage Allocater is activated, use the Storage Allocater Activation wizard to assign the LUNs to the hosts that are using them.
  - If more than one host is accessing a volume set, assign the LUNs and the involved hosts to a share group.
  - For each volume set, assign the LUNs to an associated LUN group, and assign the group to a host or share group.

Note For information about the Storage Allocater Activation wizard, see the *hp OpenView storage area manager installation guide* and online help system.

Assigning LUNs for HP-UX and Solaris VERITAS Volume Manager Storage Administrator

The VERITAS Volume Manager Storage Administrator (VMSA) software stores its configuration information in the required root disk group (rootdg). VMSA requires the presence of at least one LUN in rootdg at all times. The following guidelines apply when using VMSA and Storage Allocater:

- If VMSA is set up and using storage network LUNs in rootdg before Storage Allocater is activated, use the Storage Allocater Activation wizard to assign the LUNs to the VMSA host. If multiple LUNs are used, create an associated LUN group for the LUNs and assign the group to the VMSA host.

Note For information about the Storage Allocater Activation wizard, see the *hp OpenView storage area manager installation guide* and online help system.

Caution If you activate Storage Allocater without assigning the rootdg LUNs with the Storage Allocater Activation wizard, when the VMSA host is rebooted, it will not have access to the rootdg LUNs (since they are not yet assigned), and the VMSA server will not start. To solve this problem, use Storage Allocater to assign the rootdg LUN(s) to the host, and then start the VMSA server manually.

- If possible, do not use storage network LUNs in the rootdg volume group.
- If you need to use storage network LUNs in rootdg, HP recommends including one SCSI-attached disk in rootdg. Because VMSA requires one LUN in rootdg at all times, if you use this configuration, you will be able to remove the storage network LUNs from rootdg and unassign them, as needed.
- As with all volume groups, if you use assigned storage network LUNs in rootdg, you must remove them from rootdg before they can be unassigned.

Caution For Solaris VMSA hosts: If your root disk group contains only storage network LUNs, and you unassign all of the rootdg LUNs with the **Special Unassign** command, VMSA will not load or function properly.

ECT 2.802 Brene

ROS-Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 0201
Doc: 3701

Assigning LUNs for Windows NT stripe and volume sets

About Ftdisk

Ftdisk (Microsoft's striping and volume set driver) is a disk filter driver. Once a LUN is enabled on a machine that is running Ftdisk, the LUN can only be unassigned if Ftdisk is stopped or a special unassignment is completed. This is because Ftdisk does not release its reference to the disk.

To determine if Ftdisk is running, check its status by double-clicking the Devices icon in Control Panel. To avoid unnecessary reboots when assigning LUNs to a host, HP recommends disabling Ftdisk unless you plan to use stripe and volume sets. Disable Ftdisk to prevent it from restarting when the host is rebooted.

When using stripe and volume sets, create an associated LUN group for each set and assign all of the LUNs in the set to the group. Because a stripe or volume set cannot be used unless all of its LUNs are assigned to a host, using associated LUN groups will ensure that all of the necessary LUNs are assigned and unassigned together.

Tip If your stripe and volume sets are configured before Storage Allocater is activated, use the Storage Allocater Activation wizard to assign them to associated LUN groups, and then assign the associated LUN groups to the appropriate host(s).

Configuring stripe and volume sets

You must have Ftdisk enabled if you want to create stripe and volume sets in Disk Administrator or access these sets on a Windows NT host. Ftdisk looks for and attaches to disks when it is loaded—at system startup. If Ftdisk is not enabled when you configure sets, Disk Administrator will enable it and force a reboot.

If LUNs are assigned to a host that already has Ftdisk started, Disk Administrator, which refreshes when it starts up, will let you see them and allow you to go through the motions of creating a set. Because Ftdisk did not find the newly assigned LUNs at system startup, it will not handle the new set(s) properly, and Disk Administrator might quit unexpectedly. Or you may end up with an invalid set that appears to span several LUNs but actually includes just one.

When creating sets, HP recommends the following procedure:

1. Create an associated LUN group that contains the LUNs that will be used to create a stripe or volume set.
2. Assign the associated LUN group to the host that will be used to create the stripe or volume set.

Note For instructions on creating, editing, and assigning associated LUN groups, see the Storage Area Manager online help system.

3. Reboot the host.
4. Create the stripe or volume set. For instructions, see your Windows NT documentation.

RQS Nº 03/2005 - CN
CPML - CORREIOS
0202
Fls:
Doc: 3701

Managing LUNs with Windows 2000 dynamic volumes

If you want to create a dynamic volume (for example, a simple, spanned, striped, mirrored, or RAID-5 volume) on Fibre Channel storage, complete the following steps. If you have existing dynamic volumes before Storage Allocater is activated, use the Storage Allocater Activation wizard to assign the volumes to the appropriate associated LUN groups, hosts, and share groups.

1. For dynamic volumes that will span multiple LUNs, assign the LUNs to an associated LUN group. This will prevent the LUNs from being assigned and unassigned separately.
2. Assign the LUN (for simple volumes) or associated LUN group (for spanned, striped, mirrored and RAID-5 volumes) to a host.

Note For instructions on creating, editing, and assigning associated LUN groups, see the Storage Area Manager online help system.

3. If necessary, upgrade the assigned LUNs to dynamic disks.
4. Create the dynamic volume.

Unassigning and reassigning dynamic volumes

If you unassign a LUN or associated LUN group that contains a dynamic volume, when you reassign the LUN or associated LUN group to a host, the dynamic volume might not mount automatically.

Reassign: Same Host

If you unassigned a LUN or associated LUN group that contains a dynamic volume, and then you reassigned it to the host that created the volume, use the following procedure. If you assigned the LUN or associated LUN group to a different host, use the procedure on page 133.

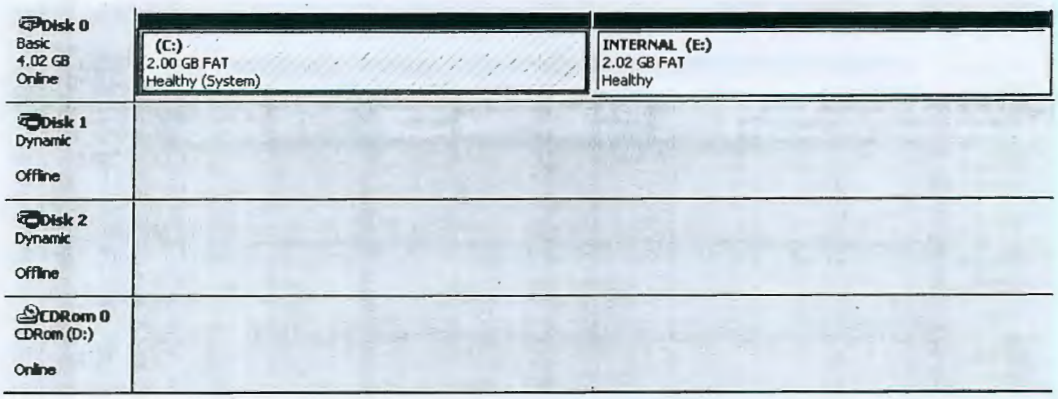
1. To open Disk Management, right-click the My Computer icon and select **Manage**.

2.798 June

2. If you are using Disk Management remotely, right-click **Computer Management (Local)**, click **Connect to another computer**, and then select the computer you want to connect to.

3. In the Computer Management window, expand **Storage** and select **Disk Management**.

   The dynamic disks will be listed with a status of **Offline**.



4. Right-click one of the disks in the volume set and select **Reactivate Disk** in the shortcut menu.

   The dynamic disks will return to **Online** status.

Reassign: Different Host

If you unassigned a LUN or associated LUN group that contains a dynamic volume, and then you reassigned it to a host other than the one that created the volume, use the following procedure.

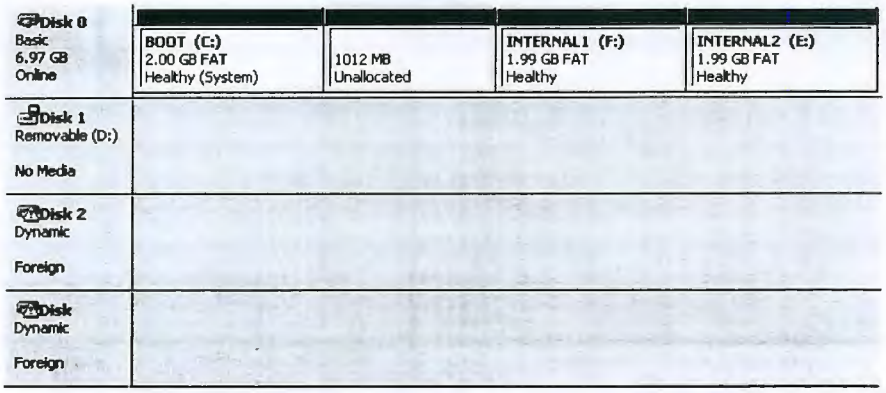
1. To open Disk Management, right-click the My Computer icon and choose **Manage**.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0203
Fls:
Doc: 3701

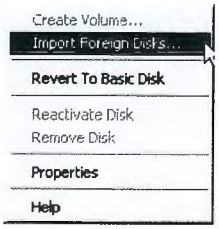
2. If you are using Disk Management remotely, right-click **Computer Management (Local)**, click **Connect to another computer**, and then select the computer you want to connect to.

3. In the Computer Management window, expand **Storage** and select **Disk Management**.

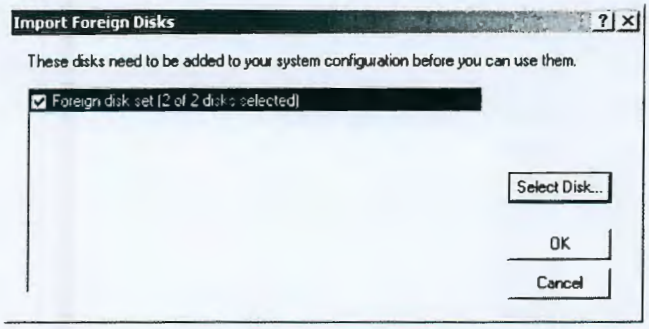
4. The dynamic disks will be listed with a status of **Foreign** because the volume was created by a different host.



5. Right-click one of the disks in the volume set and choose **Import Foreign Disks** in the shortcut menu.

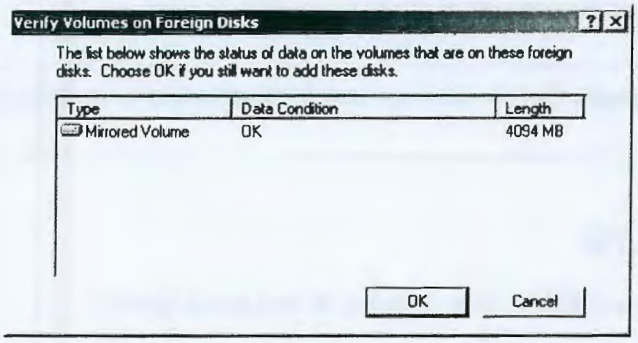


The Import Foreign Disks window appears with the foreign disks selected.



6. Click **OK**.

The Verify Volumes on Foreign Disks window lists the condition of the data on the foreign disks.



7. Click **OK**.

The dynamic disks will return to **Online** status.

Viewing assigned LUNs on HP-UX hosts

When you run **ioscan** on an HP-UX host, only the assigned Fibre Channel LUNs are listed. If no LUNs are assigned to the host, no Fibre Channel LUNs are listed. All of the targets and

ROS Nº 09/2005 - CN
CPMI - CORREIOS
0204
Fls:
3701
Doc:

always listed by their hardware path. In the following example, there are no assigned LUNs.

```
10/1/4/0                    fc                    HP Tachyon TL/TS Fibre Channel Mass Storage Adapter
10/1/4/0.8                      fcp                 FCP Protocol Adapter
10/1/4/0.8.0.255.0                      ext_bus     FCP Device Interface
10/1/4/0.8.0.255.0.0                      target
10/1/4/0.8.0.255.0.2                      target
10/1/4/0.8.0.255.0.3                      target
10/1/4/0.8.0.255.0.4                      target
10/1/4/0.8.0.255.0.5                      target
10/1/4/0.8.0.255.0.6                      target
10/1/4/0.8.0.255.0.7                      target
10/1/4/0.8.0.255.0.8                      target
10/1/4/0.8.0.255.0.9                      target
```

Assigning storage to an HP-UX host

In the Storage Area Manager user interface, assign storage to an HP-UX host.

Note See the Storage Area Manager Online Help system for instructions on assigning storage.

Listing newly assigned LUNs

To list the newly assigned Fibre Channel LUNs, type **ioscan -k** and press **Enter**.

Note When you use the **ioscan -k** command, newly assigned LUNs are listed, but the HP-UX system does not scan for LUNs that have been added to the storage network since the last **ioscan**.

When there are assigned LUNs, running **ioscan** will list the hardware paths to all of the Storage Allocater targets plus the assigned LUNs. For example:

```
10/1/4/0                fc                      HP Tachyon TL/TS Fibre Channel Mass Storage Adapter
10/1/4/0.8                fcp                   FCP Protocol Adapter
10/1/4/0.8.0.255.0                  ext_bus     FCP Device Interface
10/1/4/0.8.0.255.0.0                  target
10/1/4/0.8.0.255.0.2                  target
10/1/4/0.8.0.255.0.3                  target
10/1/4/0.8.0.255.0.3.0                  disk    SEAGATE ST118202 CLAR18
10/1/4/0.8.0.255.0.4                  target
10/1/4/0.8.0.255.0.4.0                  disk    SEAGATE ST118202 CLAR18
10/1/4/0.8.0.255.0.5                  target
10/1/4/0.8.0.255.0.6                  target
10/1/4/0.8.0.255.0.7                  target
10/1/4/0.8.0.255.0.8                  target
10/1/4/0.8.0.255.0.9                  target
```

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0205
Fls:
3701

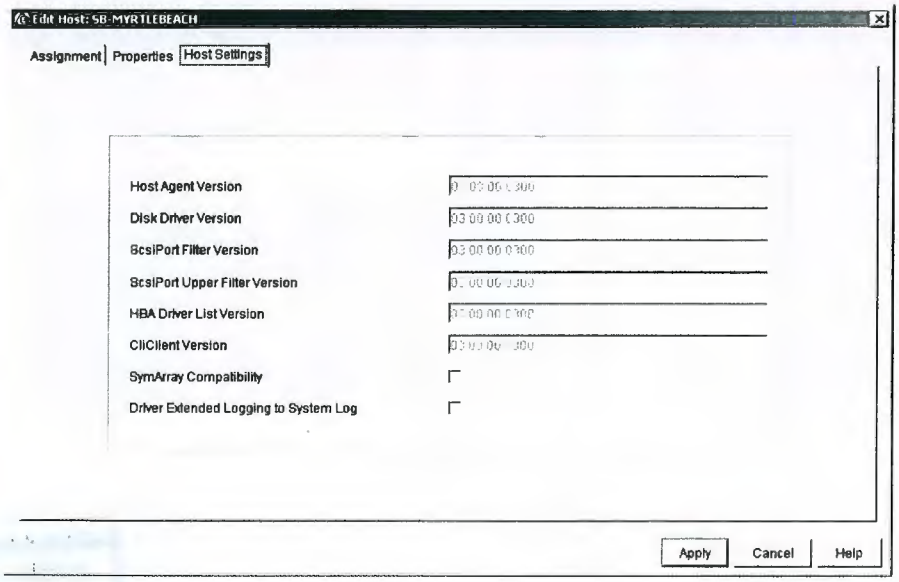
Managing hosts

Modifying Windows NT host settings

Host Settings tab

Use this procedure to edit the registry settings for HP installed services on Windows NT hosts. You can also edit the registry settings with a registry editor, as described on page 139.

1. In the Resources tree, expand **Hosts**.
2. Right-click a Windows NT host and choose **LUN Allocation**.
3. Click the **Host Settings** tab. A window similar to the following appears.



4. To toggle between enabled and disabled status for the SymArray Compatibility, Driver Extended Logging to System Log registry settings, select or clear the corresponding check box.
5. Click **Apply**.
6. Click **Close**.
7. If you changed the SymArray Compatibility setting, reboot the host to activate the changed registry setting.

Registry editor

To edit registry settings with a Windows NT registry editor, run Regedit or Regedt32 and edit the desired settings.

Caution Editing the registry incorrectly may cause serious problems that will require you to reinstall Windows NT. For more information about editing the registry, see your Microsoft documentation.

Table 3 Storage Allocater registry settings

Path:	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\trdisk
Value Name:	SymArrayCompatibility
Value Type:	REG_DWORD
Implicit Default:	0
Purpose:	To modify the behavior of Storage Allocater's TRDISK driver so it gives control of FC60 LUNs to the SymArray (RDAC) driver, whereas normally, TRDISK would control all Fibre Channel disk LUNs. Set this value to 1 to enable SymArrayCompatibility mode, which will allow RDAC failover of FC60 LUNs to work on this host.
Path:	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\trfilter
Value Name:	ExtendedLogging
Value Type:	REG_DWORD
Implicit Default:	0
Purpose:	When ExtendedLogging is enabled, a message indicating that IDs could not be created for pseudo LUNs may be generated and posted to the Windows NT event log every time the SCSI subsystem scans for devices. When ExtendedLogging is disabled, these messages will not appear. Set this value to 1 to enable extended logging.

ECT 2792 fls
ROSNI 03/2005 - CN
CPMI - CORREIOS
0206
Fls:
Doc: 5701

Moving a host from one management server to another

If you want to move a Storage Allocater host from one management server to another, you must uninstall the Host Agent software from the host, and then reinstall the Host Agent software and activate Storage Allocater from the new management server. This step is required because the Host Agent software is tied to an individual management server that is configured during the installation of the Host Agent software.

1. Unassign all storage from the host and remove the host from any share groups.
2. Detach the host from the storage network.
3. Uninstall the Host Agent software from the host.
4. In the Storage Area Manager Resources tree, right-click the host and select **Delete <host name>** on the shortcut menu.
5. If necessary, connect the host to the same LAN as the new management server, but do not attach it to the storage network.
6. Install the Host Agent software from the new management server and activate Storage Allocater as described in the *hp OpenView storage area manager installation guide.*
7. Attach the host to the storage network.

Managing a "dead" host

If a host goes offline because of a hardware failure and it cannot be brought back online to unassign its storage, use the following procedure to remove the host from the storage network.

1. Detach the host from the storage network.
2. In the Storage Area Manager user interface, right-click the host and choose **Delete <host name>**.
3. When prompted to confirm the deletion, click **Yes**. When the host is deleted, it is removed from the Storage Area Manager database, all of the storage assigned to it is unassigned (which makes it available for assignment to other hosts), and the host is removed from any groups it is assigned to.

Restoring a dead host

- If the host becomes usable, but it is not going to be reattached to the storage network, use the local uninstall procedure to uninstall the Host Agent software from the host. For uninstall instructions, see the *hp OpenView storage area manager installation guide.*
- If the host becomes usable and it is going to be reattached to the storage network and added back into the Storage Area Manager database, then it is not necessary to uninstall the Host Agent software. Just make sure that the host is not attached to the storage network until it has been added back into the Storage Area Manager database via the Ethernet network, and any potential multiple writer situations have been corrected. For more information about multiple-writer situations, see page 196.

Caution Reattaching a host to the storage network is not recommended. If the host is reattached to the storage network before it is added to the database, it will have access to any storage that was unassigned in step 3. If another host already has access to this storage, a multiple-writer situation may occur and cause data corruption.

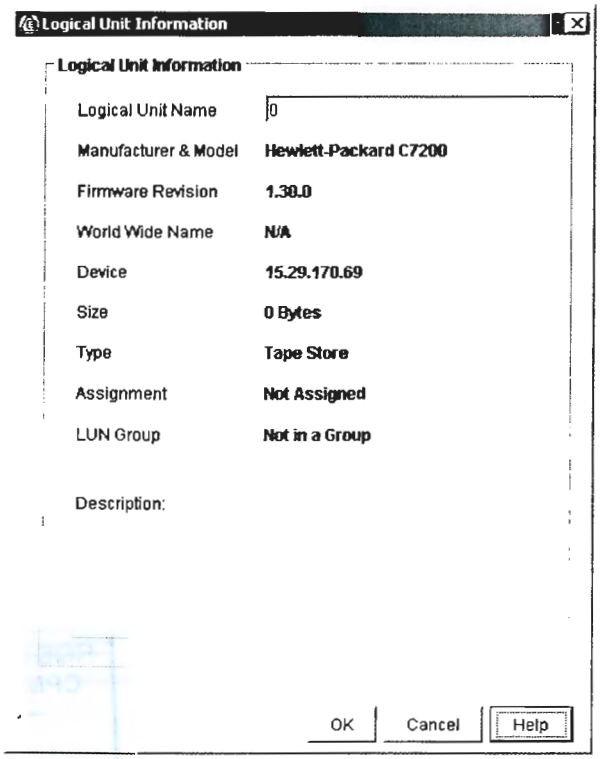
RQS Nº 03/2005 - CN
CPMI - CORREIOS
0207
Fls:
Doc:

Managing LUNs

Viewing or modifying logical unit information

Use this procedure to view or edit information about a logical unit (LUN).

1. In the Resources tree, expand **Storage Devices** and then a particular storage device.
2. Select **Logical Units** and click the **LUN Allocation** tab.
3. Select a LUN and click the **Edit Selected** button. The Logical Unit Information window appears.



The Logical Unit Information window displays the following items:

- Logical Unit Name: The LUN's name. This name is initially generated by Storage Area Manager, and can be changed in this window.
- The manufacturer and model of the storage device that contains this LUN.
- Firmware Revision: The version of the firmware on the listed LUN.
- The node world wide name of the storage device.
- Device: The name of the storage device that contains this LUN.
- Size: The capacity of the listed LUN.
- Type: The type of storage device that contains the LUN.
- Assignment: The host, associated LUN group, or share group to which the LUN is assigned.
- LUN Group: The LUN group that contains the LUN.
- Description: A description of the LUN.

4. To change the LUN's name, enter a new name in the Logical Unit Name text box
5. To change the LUN's description, enter a new description in the Description box.
6. To close the window and apply any changes to the LUN's name or description, click the **OK** button.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0208
Fls:
3701
Doc:

Viewing or deleting missing LUNs

If you are using Storage Allocater, when you delete a storage device from the Storage Area Manager database, use this procedure to delete the storage device's LUNs. If you do not delete the storage device's LUNs, they may be listed in the Edit window even though the device is no longer attached to the storage network.

1. Make sure the storage device is detached from the storage network, and then delete the storage device.
2. Wait a few minutes for the Storage Area Manager database to update.

   Although the storage device has been deleted from the database, its LUNs will still be listed in Storage Allocater's Edit window.
3. Unassign the deleted storage device's LUNs from all hosts and groups.
4. Select **Missing Logical Units** from the **Tools** menu and **Storage Allocater** submenu. The Missing Logical Units window appears with a list of all the missing LUNs and their creation and modification dates.
5. Select the missing LUNs and click the **Delete Selected** button, or click the **Delete All** button.
6. When prompted to confirm the removal of the missing LUNs, click **OK**.

2.786 June

hp OpenView storage allocater interoperability

With FC60 storage arrays

Software for managing storage devices, such as disk arrays and tape libraries, often manages them by issuing SCSI commands to management LUNs on those devices. When Storage Allocater is installed on a storage network, these commands cannot be sent to such a device unless all of the management LUNs are assigned to the host on which the software is running. The same LUNs often represent units of storage as well as management command targets, so it may be necessary to assign storage LUNs to the management host (perhaps temporarily) even though the storage is not needed on that host.

The SM60 software for HP FC60 arrays is an example of such management software. The Universal Xport LUNs from each array must be assigned to a host running the SM60 Agent service. Note that the agent host does not have to be the same host on which you run the SM60 Client GUI, because the client can administer FC60 arrays through remote agents.

FC60: Windows mode

Storage Allocater can be used with HP FC60 storage arrays and the RDAC driver included with the HP Storage Manager 60 software (SM60). SM60 is an application and agent pair that allows you to view and modify the FC60's configuration. The SM60 agent runs as a service (Storage Manager 60 Agent) on any host that is connected to the array.

RDAC is an I/O path failover driver that is installed on all host computers that access the FC60. Typically, a pair of active controllers is located in a storage array. Each logical unit in the array is owned by one controller that provides the I/O path. When a component in the I/O path to the owning controller fails, the RDAC driver transfers ownership of the volumes assigned to that controller to the other controller in the pair, allowing I/O to proceed on the other path, and preventing an I/O failure or interruption.

ROS Nº 03/2005 - CN
CPMI - CORREIOS
0209
Fls:
3701
Doc:

The communication between the SM60 agent and RDAC software and the controllers is done through a special volume (typically LUN 7) called an access volume. Although the access volume is presented as a unit having limited storage capacity, it is designed to handle only configuration command transactions, and cannot be used for standard data storage. The access volumes are listed as **Universal Xport** LUNs in the Storage Area Manager user interface.

For failover or SM60 management to work on any given host, the Universal Xport LUNs must be assigned to that host. HP recommends setting up a share group that includes the storage array controllers' Universal Xport LUNs and all of the hosts that are using that array and RDAC.

Setting Up Storage Allocater with the FC60 and RDAC

To use Storage Allocater with the FC60, complete the following setup procedure after Storage Allocater is installed and activated.

1. Assign all of the Universal Xport LUNs to an associated LUN group.
2. Create a share group.
3. Assign the associated LUN group (from step 1) to the share group.
4. Assign all of the hosts that will access the FC60 to the share group. This includes hosts that are running RDAC or the SM60 agent.

Note For more information about configuring associated LUN groups and share groups, see the Storage Area Manager online help system.

5. On Windows NT hosts only, set the SymArrayCompatibility registry value and reboot.When you use Storage Allocater with RDAC, the SymArrayCompatibility setting is required on all hosts that are connected to the storage array. For more information, see "Modifying Windows NT host settings" on page 138.

Guidelines: Windows NT and Windows 2000

- If the SM60 agent is installed and running before Storage Allocater is activated, the host will start after activation and will not be able to access any LUNs, including the Universal Xport LUNs. To solve this problem, do one of the following:
  - During the initial Storage Area Manager setup, use the Storage Allocater Activation wizard to activate Storage Allocater and assign the Universal Xport LUNs to the host.
  - After activation, assign the Universal Xport LUNs and hosts as described on page 146, and then stop and restart the SM60 agent service. On subsequent reboots, the Universal Xport LUNs will already be assigned, so you do not need to restart the SM60 agent service.
- If all of the Universal Xport LUNs are not assigned to a host that is running the SM60 agent, the agent will not start, and an event will be recorded in the system log.
- If the Universal Xport LUNs and all control/controller LUNs are not assigned to the host(s) that manage the array, Storage Optimizer will not be able to collect performance data from the FC60.

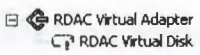
Guidelines: Windows NT Hosts Only:

- When SymArray (the RDAC driver) is used with SymArrayCompatibility enabled, if an FC60 LUN that was not assigned to a host at startup is assigned to the host for the first time, drive letters will not be created automatically for file system volumes or other partitions on the LUN. When you run Disk Administrator, the LUN is listed and displays all partitions on the disk, but no drive letters. Right-click each partition in Disk Administrator and choose **Assign Drive Letter** on the shortcut menu. The assigned drive letter(s) will be persistent across reboots as long as the LUN remains assigned to the host.
- When you assign LUNs to hosts that are using SymArray, you must unassign them with the **Special Unassign** command (page 122).

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0210
Fls:
3701
Doc:

Guidelines: Windows 2000 Hosts Only

- The FC60's access volumes (Universal Xport LUNs) are displayed as **HP Universal Xport** devices in Device Manager.
- When you assign Universal Xport LUNs to a host, the SM60 agent opens a handle to one of the LUNs. Because of this open handle, Storage Area Manager will not allow the LUN to be unassigned. To unassign a Universal Xport LUN, stop the SM60 agent service, and then unassign the LUN.
- When you unassign the last remaining FC60 LUN from a Windows 2000 host, Device Manager may mark the FC60 virtual disk with an exclamation point.



This icon badge can be ignored and will be removed with the next storage assignment or reboot.

FC60: HP-UX mode

The controller firmware for running the FC60 in HP-UX mode automatically creates a 10-megabyte management LUN (LUN 0) on a physical disk in the array. The Array Manager 60 (AM60) software uses this partition to manage the FC60.

Configuring Storage Allocater

When using Storage Allocater with an FC60 that is in HP-UX mode, assign the management LUN to a share group that contains all of the HP-UX hosts that will be used to manage the array. Individual LUNs must be managed from the hosts to which they are assigned.

Tip During the initial Storage Area Manager setup, use the Storage Allocater Activation wizard to activate Storage Allocater and assign the management LUN to a share group containing the appropriate hosts.

Note For instructions on creating and editing share groups, see the Storage Area Manager online help system.

Access to the management LUN controls the ability of AM60 command line utilities, Support Tools Manager (STM), and System Administration Manager (SAM) to display information about the FC60. Each host with access to the management LUN can see all of the FC60 LUNs in AM60, but a host can determine the status of only its assigned LUNs.

Although the management LUN uses just ten megabytes of disk space, HP does not recommend using the remaining disk space for data. In the recommended Storage Allocater/FC60 configuration, the management LUN is dedicated for FC60 management.

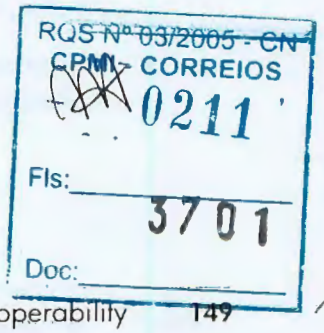
Mounting the Management LUN on an HP-UX Host

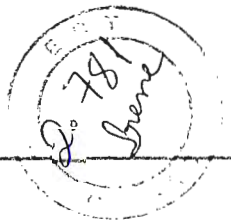
Caution Using the management LUN for data is not recommended.

If you do not want to dedicate an entire disk to FC60 management, HP-UX hosts can use the additional disk space for data. To accomplish this, grow the management LUN to fill the remaining space on the physical disk, and manage LUN access manually. Because HP-UX does not use a presented LUN until it is mounted, the management LUN can be managed by using LVM to mount it on one HP-UX host only. All of the HP-UX hosts in the share group that contains the management LUN will list the management LUN in ioscan, but will not use it if it is not mounted.

Note Do not assign the management LUN to a non-HP-UX host.

Caution Because the management LUN is in a share group, all hosts in the share group are capable of accessing the LUN. If the LUN is mounted on two or more HP-UX hosts, a multiple writer situation will occur and cause data corruption. If you want to use the remaining space on the management LUN for data, and can accept the risk and responsibility associated with managing the LUN manually, this method can be used.





Guidelines: HP-UX Hosts

- When an FC60 is used with Storage Allocater and HP-UX hosts, the **syslog** file on each HP-UX host will contain entries for FC60 LUNs that are not assigned to that host. System Administrators should monitor this file and clear entries as needed.
- If the Universal Xport LUNs and all control/controller LUNs are not assigned to the host(s) that manage the array, Storage Optimizer will not be able to collect performance data from the FC60.

With AIX cfgmgr

When Storage Allocater is installed on an AIX host, cfgmgr is affected in the following ways:

- A backup copy of /usr/sbin/cfgmgr is copied to /usr/sbin/LMcfgmgr. Do not delete the backup copy of cfgmgr.
- Storage Allocater's version of cfgmgr is copied into /usr/sbin/cfgmgr, replacing the original version.
- The system database /etc/security/sysck.cfg is updated.

Storage Allocater's version of cfgmgr is required in order to preserve LUN security on AIX hosts. If you need to install a system patch that will change cfgmgr, do the following:

1. Enter **/opt/sanmgr/hostagent/sbin/trlmcheck -prepatch**
2. Install the system patch that affects cfgmgr.
3. Enter **/opt/sanmgr/hostagent/sbin/trlmcheck -postpatch**
4. Verify that Storage Allocater's version of cfgmgr is running by entering the following command: **strings /sbin/cfgmgr | grep StorageAllocater**
   - If this command produces output, then the Storage Allocater version of cfgmgr is present, and this procedure is complete.
   - If this command does not produce output, the Storage Allocater version of cfgmgr is no longer in the /usr/sbin/cfgmgr directory. Start again with step 3.

With HP-UX ioscan

When Storage Allocater is installed on an HP-UX host, ioscan is affected in the following ways:

- A backup copy of /sbin/ioscan is copied to /sbin/LMscan. Do not delete the backup copy of ioscan.
- Storage Allocater's version of ioscan is copied into /sbin/ioscan, replacing the original version.

Storage Allocater's version of ioscan is required in order to preserve LUN security on HP-UX hosts. If you install a system update, it is possible that Storage Allocater's ioscan could be replaced by the standard version of ioscan. After updating the system software, use the following procedure to verify that Storage Allocater's ioscan is in /sbin/ioscan.

1. Run the following command: **strings /sbin/ioscan | grep StorageAllocater**.
   - If this command produces output, then the Storage Allocater version of ioscan is present, and this procedure is complete.
   - If this command does not produce output, the Storage Allocater version of ioscan is no longer in the /sbin/ioscan directory. Continue with step 2.
2. Back up the standard version of ioscan with the following command: **cp /sbin/ioscan /sbin/LMscan**
3. Use the following command to copy the Storage Allocater version of ioscan to the /sbin/ioscan directory: **cp /opt/sanmgr/hostagent/sbin/ioscan /sbin/ioscan**
4. Run **/sbin/ioscan**

With HP-UX Storage Data Protector and hp StorageWorks virtual arrays

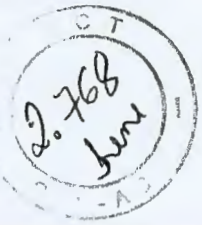
Before running a snapshot backup with hp OpenView Storage Data Protector 5.0 and a va7100, va7400, or va7410, perform the following configuration steps:

1. Using Command View SDM, create a business copy LUN for a "parent" LUN on the storage array.
2. After the business copy LUN is discovered by Storage Area Manager, assign it to the host that will perform the backup. This is the host to which the tape drive is assigned.
3. Configure Storage Data Protector for a new Snapshot backup/HP Surestore VA backup. When configuring Data Protector enable the following items in the Special Options window:
   - Use existing snapshot
   - After a successful session, leave the created snapshot

With Linux device files

For automatic mounting of file systems to work properly, a device that is mapped to a specific controller, bus, target, and LUN on a host must map to the same controller, bus, target, and LUN after the host is rebooted. Due to a limitation in the Linux SCSI subsystem, it is not guaranteed that the controller, bus, target, and LUN for a device will remain the same after a reboot. Because of this limitation, the device file that represented LUN-X before a reboot can map to LUN-Y after a reboot.

Storage Allocater for Linux handles the problem of device file persistence across reboots by creating RUID-based device file names for assigned LUNs. RUIDs provide a unique LUN ID that is independent of the unit's controller, bus, target, and LUN mapping. RUID-based device file names remain the same for a LUN even after a reboot. If you use RUID-based device file names when mounting LUNs on Linux hosts, device file persistence is ensured across reboots.



The following example shows sample commands for mounting partitions of a LUN with the standard disk driver specific device files that exist under the /dev directory:

```
mount /dev/sdd mnt/test4
mount /dev/sdd1 mnt/test5
```

The following example shows sample commands for mounting partitions of a LUN with the RUID-based device file name 931E132CR30008R700010201002R50002037112DB3-0:

```
mount /dev/trdisk/931E132CR30008R700010201002R50002037112DB3-0-1 /mnt/test1
mount /dev/trdisk/931E132CR30008R700010201002R50002037112DB3-0-2 /mnt/test2
mount /dev/trdisk/931E132CR30008R700010201002R50002037112DB3-0-3 /mnt/test3
```

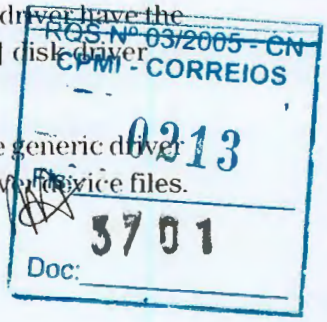
To mount file systems automatically at startup, add them to the **/etc/fstab** file. In the following example, three partitions of a LUN with the RUID-based device file name 931E132CR30008R700010201002R50002037112DB3-0 (shown in bold text) have been added to the fstab file.

```
[root@sb-iso6 trdisk]# cat /etc/fstab
LABEL=/                 /                       ext2    defaults        1 1
LABEL=/boot             /boot                   ext2    defaults        1 2
/dev/fd0                /mnt/floppy             auto    noauto,owner    0 0
none                    /proc                   proc    defaults        0 0
none                    /dev/pts                devpts  gid=5,mode=620  0 0
/dev/sda6               swap                    swap    defaults        0 0
/dev/cdrom              /mnt/cdrom              iso9660 noauto,owner,kudzu,ro 0
0
/dev/trdisk/931E132CR30008R700010201002R50002037112DB3-0-1 /mnt/test1 ext2 rw 0 0
/dev/trdisk/931E132CR30008R700010201002R50002037112DB3-0-2 /mnt/testi2 ext2 rw 0 0
/dev/trdisk/931E132CR30008R700010201002R50002037112DB3-0-3 /mnt/test3 ext2 rw 0 0
/dev/sdd                /mnt/test4              ext2 rw 0 0
/dev/sdd1               /mnt/test5              ext2 rw 0 0
```

About RUID-based device files

On Linux hosts, Storage Allocater filters all of the LUNs seen by the following Linux drivers: **sd** (disk driver), **sg** (generic driver), and **st** (tape driver).

- The RUID-based disk device files created for disk LUNs seen by the disk driver have the same characteristics as the standard **/dev/sd[a-z]** and **/dev/sd[a-z][a-z]** disk driver device files.
- The RUID-based generic device files created for generic LUNs seen by the generic driver have the same characteristics as the standard **/dev/sg[0-255]** generic driver device files.



- The RUID-based tape device files created for tape LUNs seen by the tape driver have the same characteristics as the standard **/dev/st[0-32]** and **/dev/nst[0-32]** tape driver device files.

Since the RUIDs are lengthy for certain LUNs, Storage Allocater uses a compressed form of the RUID to create device file names that fit within 256 characters. Storage Allocater's RUID-based device files are present under three Storage Allocater-specific directories: **/dev/trdisk**, **/dev/trgen**, and **/dev/trtape**. These directories contain the device files for the disk driver, the generic driver, and the tape driver, respectively.

- Any LUN that is seen by the disk or tape driver will also be seen by the generic driver.
- The generic driver may see LUNs that are not seen by the disk or tape driver, for example, media changers.

Device file names: Disk LUNs

For the disk LUNs seen by the disk driver, the **/dev/trdisk** directory contains RUID-based device files in the format <COMPRESSED_RUID>-<PATH_NO>-<PARTITION_NO> where COMPRESSED_RUID is the RUID-based file name, PATH_NO differentiates between multiple paths to the same LUN, and PARTITION_NO is a specific partition on the disk.

If you run the **ls** command under the **/dev/trdisk** directory, 15 partitions and a representation of the entire disk are listed for each Fibre Channel disk. For example:

```
[root@sb-iso4 trdisk]# ls

7541202F001R8000102010050060BR500092519002DR01006C-0

7541202F001R8000102010050060BR500092519002DR01006C-0-1

7541202F001R8000102010050060BR500092519002DR01006C-0-10

7541202F001R8000102010050060BR500092519002DR01006C-0-11

7541202F001R8000102010050060BR500092519002DR01006C-0-12

7541202F001R8000102010050060BR500092519002DR01006C-0-13

7541202F001R8000102010050060BR500092519002DR01006C-0-14

7541202F001R8000102010050060BR500092519002DR01006C-0-15

7541202F001R8000102010050060BR500092519002DR01006C-0-2
```

```
7541202F001R8000102010050060BR500092519002DR01006C-0-3

7541202F001R8000102010050060BR500092519002DR01006C-0-4

7541202F001R8000102010050060BR500092519002DR01006C-0-5

7541202F001R8000102010050060BR500092519002DR01006C-0-6

7541202F001R8000102010050060BR500092519002DR01006C-0-7

7541202F001R8000102010050060BR500092519002DR01006C-0-8

7541202F001R8000102010050060BR500092519002DR01006C-0-9
```

Device file names: Generic LUNs

For generic LUNs seen by the generic driver, which includes disk LUNs and tape LUNs, the **/dev/trgen** directory contains RUID-based device files in the format <COMPRESSED_RUID>-<PATH_NO> where COMPRESSED_RUID is the RUID-based device name and PATH_NO differentiates between multiple paths to the same LUN. There is no partition number for generic device listings because the concept of partitions does not exist for generic LUNs. When dealing with disks, generic device files always refer to the entire disk. For example:

```
[root@sb-iso4 trgen]# ls

7541202F001R8000102010050060BR500092519002DR01006C-0

76413D2F001R8000102010050060BR500092519003R11006F-0

7741R3002F001R8000102010050060BR500092519002FR01006E-0

7D41282F001R8000102010050060BR5000925190025R010064-0

5D1D2E220024R70001020108485020202020202043373230302D383030302020202020R3005339445430
303132352020-0

5E09E202R30008R7000102010100E09E6R50009D3F-0

0E209E205R30008R7000102010100E09E6R50009A83-0
```

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0214
Fls:
3708
Doc:

Device file names: Tape LUNs

For tape LUNs seen by the tape driver, the **/dev/trtape** directory contains RUID-based device files in the format [n]<COMPRESSED_RUID>-<PATH_NO> [-<DEVICE_CHARACTERISTICS>] where n is present for tape LUNs with no-rewind functionality, and n is absent for tape LUNs with rewind capability. COMPRESSED_RUID is the RUID-based device name, PATH_NO differentiates between multiple paths to the same LUN, and DEVICE_CHARACTERISTICS pertains to characteristics of the tape LUN.

Each tape LUN is represented by 8 RUID-based device file entries that correspond to the eight minor device numbers a tape device can have. For example:

```
[root@sb-iso4 trtape]# ls
5E09E202R30008R7000102010100E09E6R50009D3F-0
5E09E202R30008R7000102010100E09E6R50009D3F-0-a
5E09E202R30008R7000102010100E09E6R50009D3F-0-1
5E09E202R30008R7000102010100E09E6R50009D3F-0-m
n5E09E202R30008R7000102010100E09E6R50009D3F-0
n5E09E202R30008R7000102010100E09E6R50009D3F-0-a
n5E09E202R30008R7000102010100E09E6R50009D3F-0-1
n5E09E202R30008R7000102010100E09E6R50009D3F-0-m
```

Note

Eight RUID-based device files are created whether or not the corresponding st files exist.

For additional information about the st driver and minor numbers, see the man pages for st.

2.764
fls.

Viewing RUIDs on Linux hosts

After Storage Allocater is activated on a Linux host, and before LUNs are assigned to the host, all of the RUIDs of LUNs seen by the host are listed as DISABLED when you perform a **cat** operation on /proc/trfilter. For example:

```
[root@sb-iso4 /root]# cat /proc/trfilter
 RUID                                                              STATUS
 4741122F00100000000102010050060B0000092519001F00000000005E      DISABLED
 6441042F00100000000102010050060B00000925190009000000000007D     DISABLED
 4441132F00100000000102010050060B0000092519001E00000000005D      DISABLED
 6B413C2F00100000000102010050060B00000925190031000000000072      DISABLED
 7541202F00100000000102010050060B0000092519002D00000000006C      DISABLED
 7B412E2F00100000000102010050060B00000925190023000000000062      DISABLED
 6541052F00100000000102010050060B00000925190008000000000007C     DISABLED
 4141142F00100000000102010050060B00000925190019000000000058      DISABLED
 5041062F00100000000102010050060B0000092519000B000000000049      DISABLED
```

When a LUN is assigned to a Linux host, even if there is no visible path to the LUN, the RUID for that LUN is displayed as ENABLED in the list of RUIDs. This means that the results of a **cat** operation on **/proc/trfilter** may not reflect whether the LUN is visible to the host. If an assigned (enabled) LUN for which no physical path exists is unassigned (disabled), the RUID will be marked as DISABLED, even though the host was never able to access the LUN.

Note When a LUN is assigned to a host, but it is not visible on the host, a message appears in the Storage Area Manager event panel. For more information, see page 194.

ROS Nº 03/2005 - CN
CPMI - CORREIOS
0215
Fls:
3701
Doc:

With Linux tape LUNs

Due to limitations in the Linux SCSI tape subsystem, when you use Storage Allocater to assign and unassign tape LUNs on Linux hosts, RUID device links may not be created immediately in the **/dev/trtape** and **/dev/trgen** directories (it may take about two seconds per LUN for RUID device links to be created).

When you assign a tape library to a Linux host, the media changer always appears as a generic LUN on the Linux host, which means that the RUID-based device file entry for the changer can be found only in the **/dev/trgen** directory, not in the **/dev/trtape** directory.

With Linux 16-byte CDBs

By default, the Linux SCSI subsystem uses 12-byte command descriptor blocks (CDBs). In order to use certain third-party applications, such as Command View SDM for Linux, you must patch the SCSI subsystem to use 16-byte CDBs.

When Storage Allocater is activated on a Linux host, the Storage Allocater drivers are configured for the current CDB setting.

To support 16-byte CDBs, change the value of MAX_COMMAND_SIZE (in the scsi.h file) from 12 to 16 and rebuild the kernel.

If a Linux host's SCSI subsystem is patched for 16-byte CDB support when Storage Allocater is already active, enter the following command before rebooting with the new kernel image: **/opt/sanmgr/hostagent/sbin/trlminstall.sh -postpatch**

With Linux Command View SDM

If Command View SDM is installed on a Linux host after Storage Allocater is activated on the host, see the preceding section, "Storage Allocater interoperability with Linux 16-byte CDBs."

With Solaris HBAs

Adding or upgrading an HBA driver

When you activate Storage Allocater on a Solaris host, the installation edits /etc/driver_classes by changing the default class of the HBA driver from **scsi** to **tran_scsi**. This change is required for Storage Allocater to run properly on Solaris hosts.

Note When you activate Storage Allocater, the fcaw driver (JNI-Sbus) is removed from /etc/driver_classes.

If you install a new HBA driver, or upgrade the HBA driver on a Solaris host, Storage Allocater will not recognize the driver automatically.

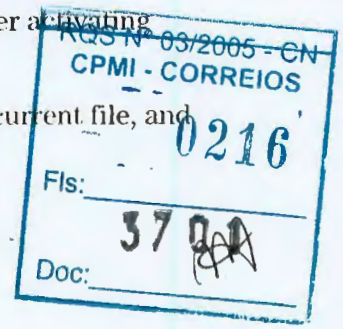
- If you are prompted to reboot after installing or upgrading a Solaris HBA driver, run the **/opt/sanmgr/hostagent/sbin/trlminstall.sh -hbaconf** script and then reboot the Solaris host.
- If you are not prompted to reboot after the HBA driver installation or upgrade, run the **/opt/sanmgr/hostagent/sbin/trlminstall.sh -hbaconf** script and then, if prompted, reboot the host.

HBA driver configuration

When you install and activate Storage Allocater on a Solaris host, the installation and activation process makes entries in the **kernel/drv/<driver_name>.conf** file, where <driver_name> is the name of your HBA driver. Later, if you run the configuration utility that came with your HBA driver, these entries may be overwritten. If this occurs, you will notice that all of the Fibre Channel storage that is assigned to the host will no longer be accessible.

HP recommends backing up the **kernel/drv/<driver_name>.conf** file after activating Storage Allocater and rebooting a Solaris host.

If assigned storage becomes inaccessible, compare the backup file to the current file, and re-enter any settings that were changed by the configuration utility.



With Solaris tape and nondisk devices

Storage Allocater's filter driver does not handle tape and other nondisk devices. To use these devices, you must configure the filter driver to allow nondisk devices to be handled by the appropriate drivers when these LUNs are assigned to Solaris hosts.

1. Open the /kernel/drv/sd_fcst.conf file.

   If LUNs have been assigned to the host, the file will be similar to the following:

```
RUIDS = "dummy"
,"68280475002800000000102020D5553534130383032333936334850202020202020
0413532333641202020202020202020202048503036"
,"765901A2000800000000102010D50060B000005A87B"
,"061E1AE70008000000001020100200000203718E626"
,"111E1AFD0008000000001020100200000203718FC31"
,"211E1AF9000800000000102010020000203718F801"
,"361E1AED0008000000001020100200000203718EC16"
,"381E1AFD0008000000001020100200000203718FC18"
,"571E1AFA0008000000001020100200000203718FB77"
,"961E1AE6000800000000102010020000203718E7B6"
,"091EBFF000080000000102010020000002037BDF129"
,"0F1EBFF800080000000102010020000002037BDF92F"
,"151EBFF000080000000102010020000002037BDF135"
,"171EBFF000080000000102010020000002037BDF137"
,"221EBFF900080000000102010020000002037BDF802"
,"651EBFF600080000000102010020000002037BDF745"
,"851EBFF800080000000102010020000002037BDF9A5"
,"AD1EBFF800080000000102010020000002037BDF98D"
,"CF1EBFF100080000000102010020000002037BDF0EF"
,"F31EBFFB00080000000102010020000002037BDFAD3"
,"C21E1AFD0008000000001020100200000203718FCE2"
;

max_luns_per_target=256;
name="sd_fcst" class="tran_scsi"
target=255 lun=0;
```

ECT 2.760 fls

The RUIDs correspond to the LUNs that are assigned to the host. If there are no LUNs assigned to the host, the file is similar to the following:

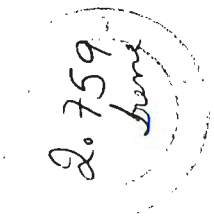
```
RUIDS = "dummy"
;
max_luns_per_target=256;
name="sd_fcst" class="tran_scsi"
target=255 lun=0;
```

2. To specify a driver to use with a particular class of devices, add a DriverSwitchTable after the semicolon that follows the list of RUIDs, and before the max_luns_per_target entry. For example:

```
RUIDS = "dummy"
;
DriverSwitchTable =
"01", "st",
"0d", "ses";

max_luns_per_target=256;
name="sd_fcst" class="tran_scsi"
target=255 lun=0;
```

The first entry corresponds to a LUN type as reported by the LUN's inquiry page, and the second entry is the installed driver that handles this type of device. In the example in step 2, **01** (tape) is the LUN type and **st** is the magnetic tape driver.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0217
Fls:
Doc: 3701



Possible values include:

00h SBC Direct-access device (magnetic disk)
01h SSC Sequential-access device (magnetic tape)
02h SSC Printer device
03h SPC Processor device
04h SBC Write-once device (some optical disks)
05h MMC CD-ROM device
06h SCSI-2 Scanner device
07h SBC Optical memory device (some optical disks)
08h SMC Medium changer device (jukeboxes)
09h SCSI-2 Communications device
0Ah – 0Bh Defined by ASC IT8 (graphic arts prepress devices)
0Ch SC-2 Storage array controller device (RAID)
0Dh SES Enclosure services device
0Eh RBC Simplified direct-access device (magnetic disk)
0Fh OCRW Optical card reader/writer device

If you install a driver for a class of devices that does not have a standard driver, you must add the driver to this list and reboot the host.

3. In order to allow a nondisk device's driver to handle an assigned LUN, force the nondisk driver to load before Storage Allocater's filter driver by editing the /etc/system file; for example, if a tape drive is assigned to the host, add the lines:

   forceload: drv/st
   forceload: drv/sd_fcst

   This will cause the system to load **st**, the tape device driver, before **sd_fcst**, the Storage Allocater filter driver.

Note If there are no forceload entries in the file, enter the appropriate information at the end of the file. If the forceload: drv/sd_fcst entry already exists, enter the nondisk driver's information above it. If the nondisk driver's entry already exists, enter the sd_fcst information after it.

4. Save the file and reboot the host.

With Solaris Omniback II, Data Protector, and tape libraries

If hp OpenView Storage Data Protector or hp OpenView Omniback II is configured to use a tape library, it installs the medium changer device driver **sst** on each Solaris host. The medium changer device is the robot arm that moves tapes from their storage slots to the tape drive for backup/restore operations, and moves them back when done.

Note To verify that the **sst** driver is installed, look for the file **/kernel/drv/sst**

To configure a Storage Allocater Solaris host so it can use Storage Data Protector or Omniback II with an assigned tape library LUN, perform the following procedure:

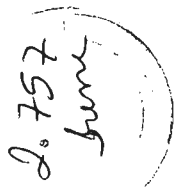
1. Open the /kernel/drv/sd_fcst.conf file.
2. Using the following values, modify the existing DriverSwitchTable. If no DriverSwitchTable exists, add one after the semicolon that follows the list of RUIDs, and before the max_luns_per_target entry:

```
RUIDS = "dummy"
;
DriverSwitchTable =
"01","st",
"08","sst";
max_luns_per_target=256;
name="sd_fcst" class="tran_scsi"
target=255 lun=0;
```

The first entry corresponds to a LUN type as reported by the LUN's inquiry page, and the second entry is the installed driver that handles this type of device. In Step 2, 01 (tape) and 08 (media changer device) are the LUN types, **st** is the magnetic tape driver, and **sst** is the medium changer device driver.

Note When using Storage Data Protector or Omniback II with Storage Allocater, **sst** is the only supported SCSI media changer device driver.

ROS Nº 03/2005 CN
CPMI - CORREIOS
0218
Fls:
3701
Doc:



3. In order to allow the nondisk device drivers **st** and **sst** to handle an assigned tape library, edit the **/etc/system** file to force the drivers to load before Storage Allocater's filter driver (**sd_fcst**). The forceload commands can be added to any section of the **/etc/system** file, but they must be in the following order:

   forceload:drv/st
   forceload:drv/sst
   forceload:drv/sd_fcst

4. Save the file and reboot the host.

With Solaris SecurePath

After Storage Allocater is active on a Solaris host, if you need to run the SecurePath configuration utility (necessary when adding new storage arrays), complete the following procedure:

1. Open the /kernel/drv/sd_fcst.conf file.

2. Using the following values, modify the existing DriverSwitchTable. If no DriverSwitchTable exists, add one after the semicolon that follows the list of RUIDs, and before the max_luns_per_target entry:

```
RUIDS = "dummy"
;
DriverSwitchTable =
"0C","cpqccl";
max_luns_per_target=256;
name="sd_fcst" class="tran_scsi"
target=255 lun=0;
```

   The first entry corresponds to a LUN type as reported by the LUN's inquiry page, and the second entry is the installed driver that handles this type of device. In Step 2, 0C (SCSI processor device) is the LUN type, and **cpqccl** is the SecurePath driver for SCSI processor devices.

3. In order to allow the nondisk device driver **cpqccl** to handle an assigned SCSI processor device, edit the **/etc/system** file to force the driver to load before Storage Allocater's filter driver (**sd_fcst**). The forceload commands can be added to any section of the **/etc/system** file, but they must be in the following order:

   forceload:drv/cpqccl
   forceload:drv/sd_fcst

4. Save the file.
5. Assign the Compaq storage array's controller LUN to the Solaris host.
6. After successfully running the SecurePath configuration utility, run **/opt/sanmgr/hostagent/sbin/trlminstall.sh -hbaconf**, which will cause Storage Allocater to reflect the new changes to the system.
7. Reboot the host.

With Windows NT Disk Administrator

Disk Administrator is the utility provided with Windows NT for managing disk partitions. It discovers the disks and partitions attached to a host only at the time that the program starts running.

Disk Administrator does not hold disks open, and the View → Refresh menu item does not actually detect the addition or removal of storage since the time Disk Administrator started. For this reason, although it is possible to change the storage assignments of a host while Disk Administrator is running, HP does not recommend doing so. For example, if a LUN is unassigned from a host, and the partitions for that LUN are changed in Disk Administrator, the program may encounter unexpected errors or exit abruptly without committing changes.

If a LUN is assigned to a host while a disk is being partitioned in Disk Administrator, the new partitions may display incorrect partition information that belongs to the newly assigned LUN. If this occurs, exit the Disk Administrator application and then start the application again.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0219
Fls:
3701
Doc:

In some cases, LUNs that have been unassigned are still listed in Disk Administrator with "Off-Line" status. This does not mean that the storage is still accessible to the host. The Storage Allocater disk driver maintains these "disks" as placeholders so Disk Administrator and other storage administration software can successfully find the disks that are still assigned.

With Windows NT Performance Monitor

Performance Monitor, an application provided with the Windows NT operating system, is a graphical tool that measures a computer's performance. The Performance Monitor disk filter driver (Diskperf) layers over disk drivers such as Storage Allocater's trdisk. All disk I/O originating in higher-level drivers and applications passes through Diskperf, which collects performance statistics and reports them to the Performance Monitor application.

Potential problems

- The filter driver is not loaded until it is enabled (`diskperf -y`) and the computer is restarted.
- The filter has to attach to the disk before the file system mounts the disk. If the file system mounts the disk first, the filter cannot insert itself between the file system and disk, so none of the file system activity is noted. For this reason, starting the Diskperf driver through Windows control panel (Devices) will not allow you to collect performance information because the file system drivers have already mounted the disk.
- The filter driver only looks for and attaches to disks when it is loaded—at startup. If LUNs are assigned to the host afterwards, the filter driver will not filter them and no performance information can be collected for them. If you want to collect performance information for assigned Fibre Channel LUNs, assign the LUNs and reboot the host.
- Storage Allocater allows you to unassign a LUN from a host with Diskperf loaded, but if you reassign the LUN to the host, Diskperf will not filter it until the host is rebooted.

With Windows NT SCSIPORT

To optimize the interaction of Storage Allocater and SCSIPORT, enter the following registry settings.

Caution Editing the registry incorrectly may cause serious problems that will require you to reinstall Windows NT. For more information about editing the registry, see your Microsoft documentation.

Path:	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Disk
Value Name:	ScanDisconnectedDevices
Value Type:	REG_DWORD
Implicit Default:	0
Recommended Value:	1
Purpose:	Modifies SCSIPORT device scan logic: Set this value to 1 to discover LUNs that exist but return "disconnected" status when queried.
Path:	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Disk
Value Name:	LunRescan
Value Type:	REG_STRING
Implicit Default:	N/A
Recommended Value:	""
Purpose:	Modifies SCSIPORT device scan logic: Set this value to "" (empty string) to cause scans to look for new LUNs on targets that have previously been scanned. Delete this value to skip the rescan behavior.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0220
Fls:
Doc: 3701

LUNs greater than 7

Windows NT's SCSIPORT driver has a limit of eight LUNs per target (numbers 0–7), which prevents Storage Allocater and other applications and drivers from seeing devices with LUNs greater than 7.

To configure SCSIPORT to support LUNs greater than 7, use the LargeLuns registry setting.

Caution Editing the registry incorrectly may cause serious problems that will require you to reinstall Windows NT. For more information about editing the registry, see your Microsoft documentation.

Path:	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\<HBA driver name>\Parameters\Device[N]
Value Name:	LargeLuns
Value Type:	REG_DWORD
Implicit Default:	0
Recommended Value:	1
Purpose:	Modifies SCSIPORT device scan logic: Set this value to 1 to scan for LUNs greater than 7.

Note The number N appended to the device name is optional. It identifies the SCSIPORT device instance (adapter) that the setting applies to. Omitting the number applies the setting to all adapters controlled by the HBA driver.

The <HBA driver name> corresponds to the file name of your HBA driver.

2865
Irene

- Capacity comparison. Click the pie chart button in Capacity view panels to view a pie chart of the relative capacity of selected resources. For example, you can compare the free space on selected hosts.
- Data export. Click the export button to save the contents of capacity graphs and pie charts in a comma-delimited (CSV) file. Using the Command Line User Interface, you can export data in CSV, XML nd HTML formats.
- File analysis. Click the report button to view reports on stale files, junk files, largest files, largest directories, and all files and directories on each and all hosts in the domain. You can modify the default reports to perform specialized functions.
- Backup assessment. Line graphs show you the space needed for full and incremental backups and the number of files modified each day.
- Secure access to administrator functions. Only administrators can set capacity thresholds, define file reports, and schedule capacity data collection and archiving.
- Command Line User Interface (CLUI). Run-line commands expedite the viewing and configuring of Storage Builder information.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0221
Fls:
3701
Doc:

2864
bene

Physical and logical space

Storage Builder displays capacity information independently for hosts, NAS devices, and storage devices, but host and device capacity are actually two views of the same space. When you view capacity on a host, you see an analysis of its file systems. File systems are logical space that is physically distributed on various storage and NAS devices. Conversely, when you view capacity on a storage device, you see the physical space that contains parts of various file systems (logical space). In figure 3, matching fill patterns show where the same space appears as logical space on a host or NAS device and as physical space on a storage device.

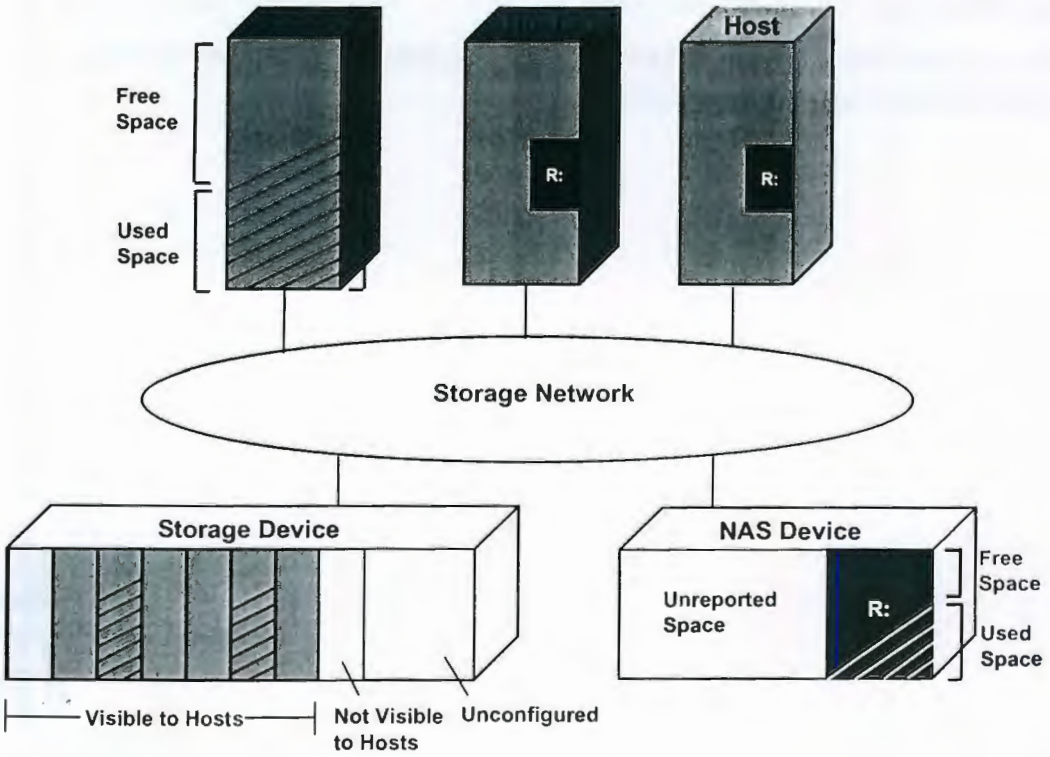


Figure 3 Physical and logical views of storage capacity

ECT 2863 Irene CPL - A

Definition of terms

The terms shown in figure 3 have the following meanings in Storage Builder:

- **Free space** is unused space in a host's or NAS device's file systems. File systems are created on physical space, but their capacity does not equal the size of the assigned physical space. Some physical space is consumed by system overhead. Also, the capacity that you see when you select a host may include file systems that reside on devices not discovered by Storage Area Manager.
- **Used space** is file system space that is occupied by files. You see used space when you select a host or NAS device and view its capacity.
- **Visible to Hosts** denotes disk or LUN space that has a physical path to one or more Storage Area Manager hosts. A host can "see" space that it does not have access to because Storage Allocater or another logical management tool has assigned the space to another host.
- **Not Visible to Hosts** denotes formatted disk or LUN space that is not reported by a Storage Area Manager host. The space may be used by hosts that have no Storage Area Manager Host Agent.
- **Unconfigured space** is raw, unformatted disk space. The term applies specifically to disk arrays, before the space is allocated to LUNs..

About NAS devices

Storage Builder discovers space on a NAS device through host data collection, but the space is reported with the NAS device. Figure 3 shows NAS device space mounted as drive R: on two hosts.

Note NAS device space must be mounted on a UNIX host to be discovered by Storage Builder.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0222
Fls:
3701
Doc:

2862
here

Capacity data collection

Storage Builder collects capacity information about storage devices, NAS devices, hosts, volumes, volume groups, directories, files, and users. All this information is typically collected several times a day and saved for as long as past data is needed, or as long as there is space for the growing database.

Storage Builder collects capacity information about storage devices, NAS devices, hosts, volumes, volume groups, directories, files, and users. Information about storage devices is collected by Storage Area Manager during the discovery cycle. All other capacity information is collected by three Storage Builder collectors deployed with Storage Area Manager Host Agents:

- The volume data collector collects the used and free space in a volume's file systems, the size of the volume, and the association of logical volumes with LUNs and volume groups on the selected host.
- The file data collector collects the size and activity of the files and directories on the selected host. File data must be collected to manage directories, report files, monitor user consumption, and determine the space needed for backups.

Note File data cannot be collected for NAS devices on Windows NT and Windows 2000 systems. NAS device capacity is reported only for volumes that are mounted on UNIX hosts.

- The user data collector identifies the users on the selected host. If the host is a domain controller or NIS (Network Information Name Service) server, all users are identified. Otherwise, only the local users are identified. The capacity associated with user accounts is collected by the file data collector.

ECT 2861 Bene

Scheduling capacity collection

Use this procedure to change Storage Builder's schedules for collecting capacity information on users, files, and volumes.

1. Select **Configure** from the **Tools** menu.

Note To edit the collection schedule for a single host, you may want to select the host in the Resources tree and click the **Configure** button in the host's Capacity view panel.

2. Select **Capacity Collection** under **Scheduling** in the Configuration tree. The Capacity Collection scheduling panel displays a list of hosts and the dates and times of the next scheduled collections on each. You can filter the list by selecting an organization in the Show Organization box.
3. Select the host(s) whose schedule(s) you want to change. (To select multiple hosts, use the Shift or Control key.)
4. Click the **Set Schedule** button at the top of the view panel.
5. Click the tab of the data collector—volume, file, or user data—that you want to change.
6. To enable or disable collection of the selected data, click the **Enable Data Collection** check box. Enabling data collection activates other text boxes in the window.
7. Once collection is enabled, specify the hours of collection as follows:
   - Enter the hour (0 through 24) and the minute (0 through 59) of the first collection of the day in the Start at boxes.
   - For periodic collections until the end of the day, check the Repeat box, and in the box at the right enter the number of hours that will elapse between each collection.
8. In the Collection Days section, select each day of the week that data will be collected. The hours specified in Collection Hours will apply to each day you select.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0223
Fls: 3701
Doc:

Note Whenever you want to return the settings to the factory defaults, click the **Restore Defaults** button.

9. To change another capacity collection schedule for the same host, click its tab and repeat steps 6 through 8.
10. When you are satisfied with the volume, file, and user data schedules, click **OK** in the Edit Collection Schedules window.
11. Click the **Apply** button in the Capacity Collection scheduling panel to implement your schedule changes and continue scheduling collection for other hosts, or click **OK** to apply your changes and close the Configuration window.

Collecting interim capacity data

Use this procedure to pre-empt the collection schedule and collect capacity data immediately on a selected host. The procedure displays the Start Hostagent Data Collection window and allows you to choose which type of data to collect:

Data will appear in Capacity view panels after it is collected and stored in the database. Depending on the amount of data requested and other factors, this may take awhile.

Note If the host or Host Agent is unavailable, or if the capacity data collector is busy when you attempt to start collection, a Storage Builder event will alert you that data collection failed to start. You should check the status of the Host Agent and the Storage Builder data collectors on the specified host.

1. Select **Configure** from the **Tools** menu.
2. Select **Capacity Collection** under **Scheduling** in the Configuration tree. The Capacity Collection scheduling panel displays a list of hosts and the next scheduled collections on each. You can filter the list by selecting an organization in the Show Organization box.
3. Select the host(s) that you want to collect data from. (Use the Shift or Control key to select multiple hosts.)

2.752
June

7 CONFIGURING THE BRIDGE

hp OpenView storage area manager bridge

User accounts

Multiple management servers

SSL

Changing the default port

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 169 0224
Doc: 3701

hp OpenView storage area manager bridge

hp OpenView Storage Area Manager Bridge, called the Bridge in the rest of this chapter, is an HTTP server that gives other applications access to Storage Area Manager data and functions (see figure 6). It is automatically installed with Storage Area Manager and runs continuously with other Storage Area Manager services on the management server. You can see the Bridge in Windows' list of services accessed from Control Panel.

With this release (Storage Area Manager 3.0), the Bridge handles requests for consolidated Storage Area Manager data from the following applications:

- hp OpenView Operations (UNIX and Windows)
- hp OpenView Reporter
- hp OpenView Service Desk

Data is returned to the requesting application in XML format.

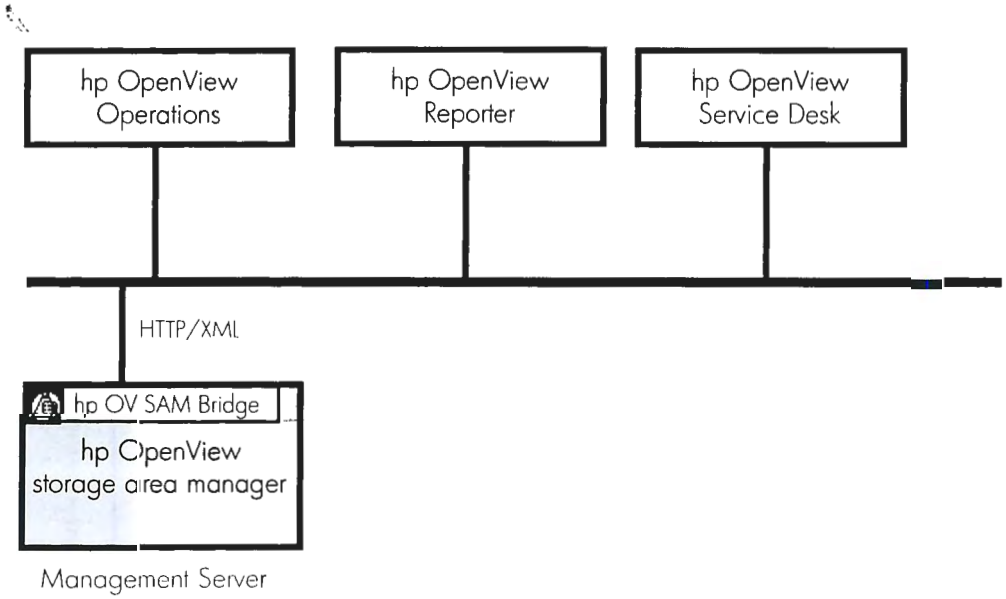


Figure 6 hp OpenView storage area manager Bridge topology

2.750 June

User accounts

Storage Area Manager requires the Bridge, and the applications using it, to log in with a user name and password. HP recommends that you set up a Storage Area Manager user account specifically for the Bridge and supply the user name and password to the person responsible for configuring an application to communicate with Storage Area Manager. A guest (read-only) account is sufficient for the currently supported applications.

If there are multiple management servers (see "Multiple management servers") in your environment, you will need to create the same user account(s) on each.

Creating Bridge user accounts

Select **Configure Security** from the Storage Area Manager **Tools** menu and click the **New User** button to create a user account. For additional information, see the online Help topic "Adding Storage Area Manager users," or click the **Help** button in the Administer Users window.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0225
Fls:
3701
Doc:

Multiple management servers

In environments with multiple management servers, one Bridge handles all external requests for all management servers (see figure 7).

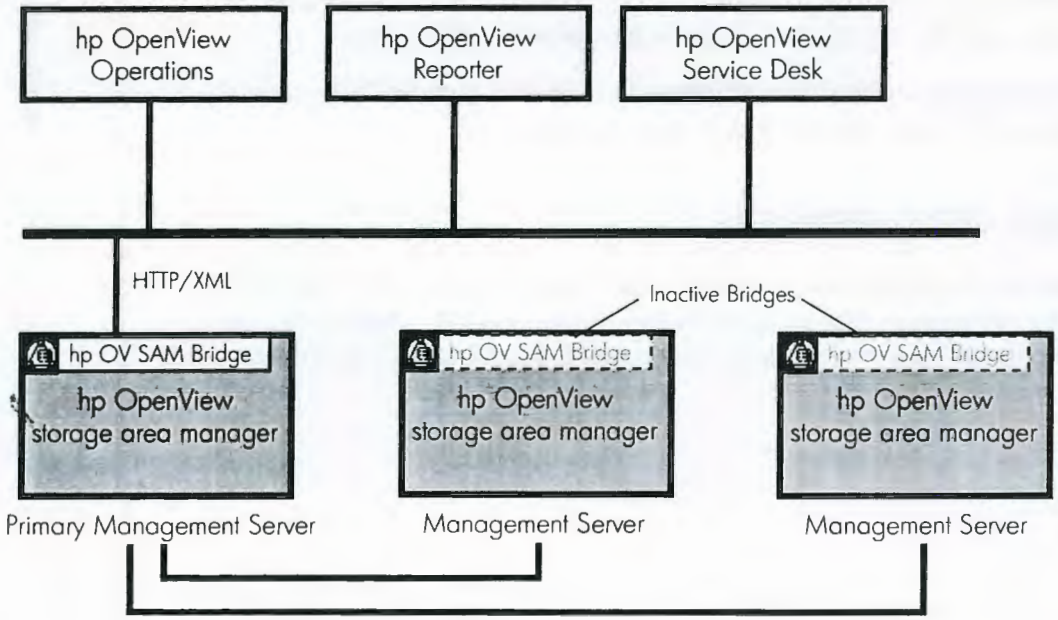


Figure 7 hp OpenView storage area manager Bridge with multiple management servers

After you choose the primary management server, there are three things to do:

1. Authorize the primary management server as a client on the other management servers (see instructions on page 173).
2. Modify the Bridge configuration file on the primary management server (see page 173).
3. Be sure that the Bridge user names and passwords are the same on all management servers (see "User accounts" on page 171).

Authorizing the primary server as a client

Enter the IP address of the primary management server in the authorizedClients.dat file at <install directory>\sanmgr\managementserver\config\ on each management server that the Bridge will contact. See "Allowing access to the management server," in chapter 2 of the *hp OpenView storage area manager installation guide* for complete instructions.

Alternatively, you can use a web browser on the primary management server to connect to the other management servers' GUI download port (http:\\<IPaddress>:8040), and click **Add your client's IP Address to the authorizedClient access list** at the bottom of the page.

Modifying the Bridge configuration file

1. On the primary management server, select Windows **Control Panel** and open **Services**.
2. Select **HP OpenView SAM Bridge** in the list of services, and then select **Stop** from the **Actions** menu.
3. Open the file <installdirectory>\sanmgr\bridge\config\SAMBridge.cfg and find the key `CONFIGURED_MANAGEMENT_SERVER_LIST`.
4. Modify this line so that it contains a comma-separated list of all of the management servers that the Bridge will contact with external requests. The default is "localhost," the Bridge's own management server. Here is an example of a modified line:

   ```
   CONFIGURED_MANAGEMENT_SERVER_LIST = localhost,ms1,ms2,ms3
   ```

   Where *ms1*, *ms2*, and *ms3* are the DNS names or IP addresses of the management servers that will accept requests from the Bridge.

Note Do not include spaces in the list.

5. Return to **Control Panel** and restart the HP OpenView SAM Bridge service.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0226
Fls:
3701
Doc:

SSL

The Bridge supports SSL (Secure Sockets Layer) for applications that require encrypted communications. These applications will obtain a server certificate from the Bridge before they trust the Bridge with encrypted information. Configuring the Bridge to use SSL involves the following steps:

1. Create a server keystore and server certificate.
2. Modify the Bridge configuration file. The SSL key must be activated to enable encrypted communication.
3. Establish a method of providing the certificate to external applications.

These steps are described below.

Creating a server keystore and certificate

A script for creating server keystores and certificates is installed with Storage Area Manager. These certificates are valid for one year, after which they can be modified for an extended period or replaced. Refer to the Java "keytool" documentation at http://java.sun.com/j2se/1.3/docs/tooldocs/win32/keytool.html for Windows 2000.

The script takes four parameters when run and prompts for SSL passwords in progress. The result is a server keystore and server certificate, the latter exported and saved as "bridgeServerCertificate.cer."

2.746
Fls.

Procedure

1. Locate the script <installdirectory>\sanmgr\bridge\sbin\createServerCertificate.bat.
2. Run the script, providing the following parameters:
   - [common name] The DNS name of the machine that the Bridge is running on.
   - [locality] The name of the city where the machine is located. Surround multiple-word values with quotation marks(" ").
   - [state] The state or province where the machine is located. You can use the full or abbreviated name.
   - [countrycode] The two-letter country code.

   For example:

   D:\sanmgr\bridge\sbin>createServerCertificate sb-apollo "Santa Barbara" CA US
3. When prompted, enter a keystore password. Applications will use this password to access the keystore. You will need to supply the same value for the `SSL_KEYSTORE_PASSWORD` key in the Bridge configuration file.
4. When prompted, enter a certificate password. Enter a password or, to use the same password as the keystore password, press **Enter**. You will also supply this value for the `SSL_PRIVATE_KEY_PASSWORD` key in the Bridge configuration file.
5. When prompted again for the keystore password, enter the password that you gave in step 3. The script needs this password to export the certificate.

When the script ends, there will be a keystore file (bridgeserver.jks) and a server certificate file (bridgeServerCertificate.cer) at <install directory>/sanmgr/bridge/config/certs.

SSCOS N° 173/2005 - CN
CPMI - CORREIOS
0227
Fls:
3701
Doc:

Sample run

The following example uses the same password for the keystore and keypass.

```
C:\sanmgr\bridge\sbin>createServerCertificate sb-apollo Santa-Barbara CA
US

When prompted, enter a keystore password and a keypass. The keypass will
protect the private key in the keystore.

Make a note of the keystore and keypass passwords. You will be prompted to
enter the keystore password in order to export the public-key certificate
from the keystore. Both passwords are needed when configuring "Bridge" to
use SSL.

Please wait...

Creating keystore and certificate

Enter keystore password: poseidon


Enter key password for <bridgeserver>

        ( RETURN if same as keystore password):

Exporting the certificate...

You will be prompted to enter the keystore password.

Enter keystore password: poseidon

Certificate stored in file <..\config\certs\bridgeServerCertificate.cer>
```

Modifying the Bridge configuration file

1. On the primary management server, select Windows **Control Panel** and open **Services**.
2. Select **HP OpenView SAM Bridge** in the list of services and then select **Stop** from the **Actions** menu.
3. Open the file <installdirectory>\sanmgr\bridge\config\SAMBridge.cfg.
4. Find the key `SSL` and enter the value **on**, to activate SSL, or **off**, to postpone the implementation of the remaining SSL options. Values are case sensitive.

2.744

5. Find the keys `SSL_KEYSTORE_PASSWORD` and `SSL_PRIVATE_KEY_PASSWORD`, and enter the values that you supplied when you ran the script and created the certificate (see above).
6. Find the key `SSL_ENCRYPTION_LEVEL` and enter one of the following values:
   - **None**. Requests will be authenticated but not encrypted.
   - **Export**. The Bridge will accept requests that use encryption methods with key lengths up to 56 bits.
   - **Full**. The Bridge will accept requests that use encryption methods with key lengths of 128 bits.
   - **Best**. The Bridge will accept requests that use the better encryption method, export or full, that the requesting application supports.
7. Find the `SSL_KEYSTORE_FILE_PATH` and enter the fully qualified path to the keystore file (bridgeserver.jks).
8. Return to **Control Panel** and restart the HP OpenView SAM Bridge service. After the service is started, the Bridge will accept only HTTPS requests.

Distributing server certificates

How external applications obtain a server certificate from the Bridge depends on the application. One way to facilitate the transaction is to establish a shared directory on a file server for every server certificate that is created. Then, whoever is configuring an application to communicate with Storage Area Manager has on hand in the shared directory all the certificates that he or she needs.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0228
Fls:
3681

Changing the default port

The default port for external applications connecting to the Bridge is 8041. If your environment requires it, you can change the port in the Bridge configuration file.

1. On the management server, select Windows **Control Panel** and open **Services**.
2. Select **HP OpenView SAM Bridge** from the list of services, and then select **Stop** from the **Actions** menu.
3. Open the file <installdirectory>\sanmgr\bridge\config\SAMBridge.cfg.
4. Find the key `PORT` and enter the number of the port where the Bridge will be monitoring third-party requests.
5. Return to **Control Panel** and restart the HP OpenView SAM Bridge service.

8 TROUBLESHOOTING

hp OpenView storage accountant

hp OpenView storage builder

hp OpenView storage builder

hp OpenView storage allocater: All platforms

hp OpenView storage allocater: Windows

hp OpenView storage allocater: HP-UX

hp OpenView storage allocater: Solaris

hp OpenView storage allocater: Linux

hp OpenView storage allocater: AIX

RDC Nº 03/2005 - CN
CPMI - CORREIOS
0229
Fls:
3701
Doc:

When the management server stops

Use this procedure to determine if the management server was not running at any time during a specified billing period. Billing information is not collected while a management server is down, and Storage Accountant fills in gaps between data collections based on the previous state. Although no billing transactions can occur while a management server is down, external events can affect an organization's access to billed storage with no corresponding indication in the bill.

A stopped management server may also explain the absence of expected entries, including data collection cycles, in the audit log.

1. On the management server, navigate to <install directory>\sanmgr\managementserver\logs.
2. Look in the logs directory for a series of files named ConJCoreMain0.log and ConJCoreMain0_x.log, where "x" indicates the numerical sequence of the file. A ConJCoreMain0_x.log was created each time the management server started or restarted. ConJCoreMain0.log is the most recent instance, that is, the file that was created when the management server last started.

Note The loggers.prp file specifies the maximum number of ConJCoreMain0_x.log files that will be maintained concurrently. The default is 4.

3. Using Notepad or another basic text editor, open the ConJCoreMain0.log or ConJCoreMain0_x.log file that was created in the specified billing period and examine the beginning of the file for the date and time of Logger Started. This is the date and time that the management server started. For example, "2001.08.17 at 09:41:31.295 Logger Started" indicates that the management server started on August 17, 2001, at 9:41 and 31 seconds am.

4. Open the last ConJCoreMain0_x. file that was created before the file you opened in step 3. Examine the end of the file for the date-time stamp of the last entry. This is the date and time that the management server stopped. For example, "2001.08.13 14:55:25.789" indicates the management server stopped on August 13, 2001, at 2:55 and 26 seconds pm.

5. Repeat steps 3 and 4 for each ConJCoreMain0_x.log file that was created or closed within the specified billing period. The difference between the date and time the logger started in one file and the date and time of the last date-time stamp in the previous file is the period during which the management server was down. In the previous examples, the management server was down from August 13, 2001, 2:55 pm, to August 17, 2001, 9:41 am.

ERQS 18103/2005 / CN
CPMI - CORREIOS
0230
Fls:
3701
Doc:

Events do not appear in the event panel

Symptom	**Cause**/Solution
Storage Accountant events are not displayed in the event panel.	**By default, Storage Accountant does not display events in the event panel.** Define an event trigger specifying the events that you want to display in the event panel.

2.738
June

Accounting screens do not show a currency symbol for fiscal data

Symptom	**Cause**/Solution
Storage Accountant screens do not show a currency symbol for fiscal data	**You have not selected a currency format for Storage Accountant.** Use one of the following solutions: – If the Setup Assistant is still open, complete the **Select Accountant Currency** step. – If the Setup Assistant is no longer available, you will be prompted to select a currency format when you create a service level.

ROS-1863/2005 - CN
CPMI - CORREIOS
0231
Fls:
3701
Doc:

Old bills are missing in the bill and report viewers

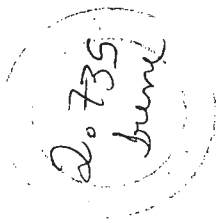
Symptom	Cause/Solution
Old bills are missing from the bill and report viewers	**The old bills were deleted according to your bill retention schedule.** See the online help topic "Archiving and restoring bills" for instructions on restoring old bills.

2736
Bunt

An error message appears when you create a new account or service level

Symptom	**Cause**/Solution
When creating a new account or service level, the message `The ID entered is not unique` appears, but the user interface does not list an account or service level with the ID that you entered.	**Account IDs must be unique across all organizations, and the IDs of closed accounts cannot be reused. Service level IDs must be unique, and IDs of deleted service levels cannot be reused.** Make sure that you enter a unique ID that was not used for a closed account or deleted service level.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0232
Fls:
3701
Doc:



hp OpenView storage builder

A managed directory has zero used space

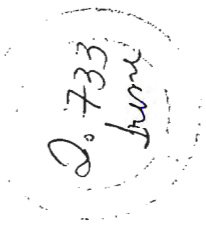
Symptom	**Cause**/Solution
A managed directory erroneously appears with 0 (zero) used space or size in the Managed Directories view panel.	**The directory was added using the CLUI but the name was entered with a different case than was used when the directory was created.** Add the directory using the GUI. (See "Adding managed directories" in chapter 3 of this guide.) When you use the CLUI to add the directory, first run **dir** (or its UNIX equivalent) in a command window on the affected host and verify the case that was used when the directory was created. Then add the directory, being careful to match upper and lowercase letters.

2734

Data is unavailable in the Add Directories window

Symptom	**Cause**/Solution
Instead of volumes and directories, you see "data unavailable" in the directory tree.	**Volume or file data has not been collected.** Verify that data collection is scheduled. View the collection schedule for volume and file data. Both must be enabled and have completed at least one cycle before directory information can appear. In addition, volume data must be collected before file data can be collected. If volume data has not been collected, no volumes will appear in the Add Directories window. If volume data has been collected but file data has not, you will also see an error message when you attempt to open a volume in the Add Directories window.
	There was a collection error. Use the default Capacity filter to check the Storage Area Manager event panel for events indicating that collection failed or failed to start on the specified host, that volumes could not be resolved with LUNs, or that LUNs could not be resolved with a host device file. If a collection error occurred, make sure that the host is reachable, that the Host Agent is running, and that the host has access to the management server.
"Network error" appears in the directory tree.	**The client was unable to retrieve the data from the management server.** An error on the management server prevented Storage Builder from processing data that was obtained from the host. There may have been a temporary communication problem between the client and management server. Close the Add Directories window and click the **Add Directories** button again.
A subdirectory does not appear in the directory tree. Also, no files are listed for the parent directory in capacity reports.	**Storage Builder does not have read access to the parent directory.** Make sure the parent directory allows read access.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0233
Fls:
3701
Doc:



There is no Capacity tab

Symptom	Cause/Solution
The view panel for collective or specific hosts, storage devices, NAS devices, or organizations contains no Capacity tab.	**hp OpenView Storage Builder was not purchased or installed.** Verify that Storage Builder is installed. Click the **Help** menu and select **About hp OpenView storage area manager**. Make sure that the current Storage Builder version is listed with the other Storage Area Manager applications.
	The Storage Builder license is out of compliance. Verify that the license to use Storage Builder is current. Click the **Tools** menu and select **Configure**, and then select **Licensing** from the Configuration tree. The Licensing view panel lists the current licenses and their expiration dates.
	Storage Builder does not support the selected resource. Verify that Storage Builder supports the specific resource(s). Click the **Help** button and select **Installation Guide Online** to view supported devices in the *hp OpenView storage area manager 3.0 installation guide*.

There is "no data" in a performance list or chart

Symptom	Cause/Solution
"No Data" appears in the metric column of a performance list, or a performance chart is empty and "No Data" appears with the metric name.	**The specified time period is outside the range of collected data.** Verify that data should have been collected during the displayed time period. In performance lists, the time period is identified in the toolbar. In performance charts, the dates on the x-axis identify the time period. If you cannot validate the displayed time period, change the time period to more reliable dates. See "Changing the displayed time period" in the Storage Area Manager online help system.
	Supporting software is not installed or not running. Check Storage Area Manager's event panel for the events "Tool used for collection of performance data on <resource name> is not installed" or "Tool used for collection of performance data... is not running." If either event occurred, troubleshoot the status and configuration of Storage Optimizer's source of performance data on the resource. On a host, for example, make sure that OpenView Performance Agent or VantagePoint is installed and running.
	The resource or path to the resource is down. Check Optimizer-DataCollector.log on the management server for exceptions that indicate a problem communicating with the resource. Troubleshoot the status of the resource, connecting devices, and physical links.
	The management server is in a conflicting state. Check Storage Area Manager's event panel for events that indicate collection or summarization did not occur because a comprehensive discovery was running or because Storage Optimizer was still storing data from a previous collection. Collection will occur at the next scheduled interval.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0234
Fls: 3701
Doc:

There is no Performance tab

Symptom	Cause/Solution
The view panel for collective or specific hosts, interconnect devices, or storage devices contains no Performance tab.	**hp OpenView Storage Optimizer was not purchased or installed.** Verify that Storage Optimizer is installed. Click the **Help** menu and select **About hp OpenView storage area manager**. Make sure that the current Storage Optimizer version is listed with the other Storage Area Manager applications.
	The Storage Optimizer license is out of compliance. Verify that the license to use Storage Optimizer is current. Click the **Tools** menu and select **Configure**, and then select **Licensing** from the Configuration tree. The Licensing view panel lists the current licenses and their expiration dates.
	Storage Optimizer does not support the selected resource. Verify that Storage Optimizer supports the specific resource(s). Click the **Help** button and select **Installation Guide Online** to view supported devices in the *hp OpenView storage area manager 3.0 installation guide*.

hp OpenView storage allocater: All platforms

LUNs are not listed in the Available to Assign list

Symptom	Cause/Solution
When editing a host or share group, LUNs are not listed in the Available to Assign list.	**By default, only visible LUNs are listed in the Available to Assign list.** Click the **Find** button, check the **Show All** checkbox, and click **OK**.

Note A LUN is visible to a host when the host has a physical path to the LUN. When editing a share group, a LUN is considered visible if at least one host in the share group has a physical path to the LUN.

Your storage has not been discovered by Storage Area Manager. To verify that the missing LUNs have been discovered, check to see if they are listed under **Storage Devices** in the Resources tree.

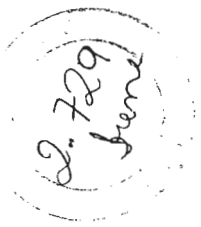
- If the storage has not been discovered, choose **Start Comprehensive Discovery** from the **Tools** menu.
- If this does not work, or if you brought the storage online after all of the hosts were started, run the **LUN Discovery** command on at least one host, and then choose **Start Comprehensive Discovery** from the **Tools** menu.

To run the LUN Discovery command, right-click a host and select **LUN Discovery** on the shortcut menu.

Note For more information about adding storage and LUN Discovery, see the "Adding New Devices" and "LUN Discovery" topics in the Storage Area Manager online help system.

Your storage device is not supported with Storage Allocater. Verify that you are using supported storage devices.

ECT Nº 03/2005 - CN
CPMI - CORREIOS
0235
Fls: 3701
Doc:



LUN Allocation and LUN Discovery do not appear in the user interface

When you right-click a host in the Storage Area Manager user interface, the LUN Allocation and LUN Discovery commands are not in the shortcut menu.

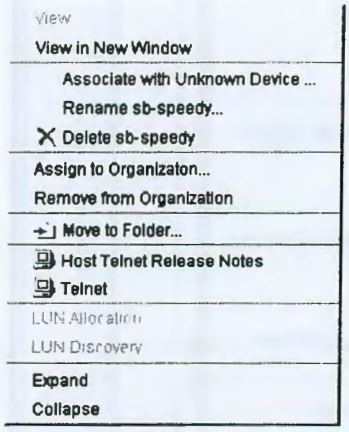
Symptom	**Cause**/Solution
When you right-click a host, LUN Allocation and LUN Discovery do not appear in the shortcut menu.	**Storage Allocater is not active on the selected host.** Activate Storage Allocater on the host. For instructions, see the *hp OpenView storage area manager installation guide.*
	After the createnewdb.cmd command was run, the Host Agent service (Windows NT, Windows 2000) and processes (Unix) were not restarted. You must restart the Host Agent services and processes on each host after using the **createnewdb** command.

Note If this problem occurs after migrating from Storage Area Manager 2.1 or later, see chapter 4 of the *hp OpenView storage area manager installation guide.*

2.726
Jun

LUN Allocation and LUN Discovery are disabled in the user interface

When you right-click a host in the Storage Area Manager user interface, the LUN Allocation and LUN Discovery commands are disabled in the shortcut menu.



Symptom	**Cause**/Solution
When you right-click a host, LUN Allocation and LUN Discovery are disabled in the shortcut menu.	**The selected host required a reboot after Storage Allocater was activated, and was not rebooted.** Reboot the host.

RG 190 03/2003 - CN
CPMI - CORREIOS
0236
Fls:
3701
Doc:

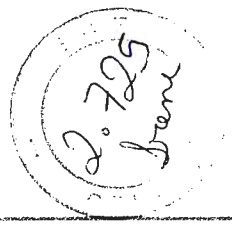
Assigned LUNs are not available on a host

If an assigned LUN is not visible to a host, find the cause below that best describes the situation, and then attempt the solution. When this occurs, the following message appears in the event panel: `Host <host name> has one or more LUNs enabled which are not reachable from that host.`

Symptom	**Cause**/Solution
Assigned LUNs are not available on a host.	**The host bus adapter (HBA) or driver are not installed.** Install the HBA or HBA driver.
	SAN-attached storage or other network hardware is turned off. Turn on the drives or network hardware.
	Network cables are not connected properly. Verify all cable connections.
	There is a failure within the Fibre Channel loop. Turn off the Fibre Channel hardware, and then turn on the hardware to reset the Fibre Channel loop.
	The Fibre Channel card has become unseated in the computer. Shut down the computer, and remove and reseat the card.
	The Fibre Channel card, hub, switch, or storage controller is bad. Run device- and vendor-specific diagnostics and replace any bad components.
	The host has not discovered the LUN. Try the following solutions: – Verify that there is a physical path between the host and the storage. – Verify that the storage network is not intentionally configured (with Storage Allocater, fabric zoning, or storage device security) to prevent the host from accessing the LUN. – In the Storage Area Manager user interface, right-click the host and select **LUN Discovery** on the shortcut menu.

Symptom	Cause/Solution
Assigned LUNs are not available on a host (cont'd)	**On Solaris hosts, if some assigned LUNs are not accessible, the sd_fcst .conf file may not be configured to search for all of the LUNs on the storage network.** Change the max_luns_per_target value in the sd_fcst.conf file to the largest number of LUNs that are configured on any disk array on your storage network.

RQS N 03/2005 - CN
CPMI - CORREIOS
0237
Fls:
3701
Doc:



A multiple writer situation is detected

If Storage Allocater detects multiple hosts with access to the same LUN the following message is posted in the event panel: `Logical Unit <logical unit name> is enabled on Host <host name>. Yet the Logical Unit indicates that it is assigned to <host or group name>. This possibly is a multiple writer situation. Storage Area Manager will try to unassign the Logical Unit from the Host.`

Symptom	**Cause**/Solution
Storage Area Manager detects a multiple writer situation.	**Storage Allocater has detected a multiple writer situation.** This occurs in the following situation: 1. A host (Host 1) with assigned LUNs is deleted in the Storage Area Manager user interface and detached from the storage network. Any LUNs that were assigned to the host are now available for assignment. 2. You assign one of the LUNs to a second host (Host 2). 3. Host 1, which still has the Host Agent software installed, is reattached to the storage network and rebooted. At this point, Storage Allocater tries to unassign the LUN from Host 1. One of the following messages is displayed in the event panel: – `<logical unit name> has been removed from <host name>. The multiple writer situation has been resolved.` If this message appears, the LUN has been unassigned from Host 1 and will be assigned to Host 2. – `<logical unit name> has not been removed from <host name>. The multiple writer situation still exists!`

Symptom	Cause/Solution
Storage Area Manager detects a multiple writer situation (cont'd).	4. If the LUN is in use by Host 1 and cannot be unassigned, Storage Allocater posts the following message in the event panel: `Storage Area Manager will attempt to remove Logical Unit <logical unit name> from <host or group name> to resolve the possible multiple writer situation` and tries to unassign the LUN from Host 2. One of the following messages is displayed in the event panel: – `<logical unit name> has been removed from <host or group name>.` The multi-writer scenario has been resolved. If this message appears, the LUN will be assigned to Host 1. – `<logical unit name> has not been removed from <host or group name>. The multiple writer situation still exists!` If Storage Allocater cannot resolve the multiple writer situation, take Host 1 off the storage network, but leave it on the LAN. Reboot Host 1, and the affected LUN will be unassigned from Host 1, and it will remain assigned to Host 2.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0238
Fls:
Doc:
3701

hp OpenView storage allocater: Windows

A LUN cannot be unassigned from a Windows host

If a LUN cannot be unassigned, a failure message will appear in the Configuration Status window and in the event panel on the management server.

Symptom	**Cause**/Solution
A LUN unassignment fails.	**There are open files or folders, or volumes on the LUN.** Shut down any applications, services, or third-party drivers that may be holding open files, folders, or a volume.
	The file server is sharing a volume or folder on the LUN. Log off remote clients and stop sharing the volume or folder.
	On a Windows NT host, Ftdisk is running. Try the following solutions: – Use the **Special Mode Unassign** command to unassign the LUN, and restart the host. – Use the Windows Control Panel (Devices) to disable Ftdisk and reboot the host. Note that stripe- and volume-sets will not be accessible with Ftdisk disabled.
	A disk filter is running. Try the following solutions: – Use the **Special Mode Unassign** command to unassign the LUN, and restart the host. – Determine which disk filters are running and deactivate them if they are not being used. Restart the host after deactivating any disk filters.

Symptom	Cause/Solution
A LUN unassignment fails (cont'd).	**A software crash or operating system resource leak can leave open handles to a LUN.** Use the **Special Mode Unassign** command to unassign the LUN, and restart the host.
	A service or SNMP agent is preventing the LUN unassignment. Services are configurable under the Services control panel and SNMP agents are loaded by the SNMP service. Disable unneeded storage-related services and SNMP agents. If a needed service or agent is causing the problem, use the **Special Unassign** command.
	When a nondisk LUN for which no driver can be found is assigned to a Windows 2000 host, a sequence of events can leave the LUN in a state that prevents it from being unassigned. **Note** This state can be determined by viewing the LUN in Device Manager, where its icon will be a yellow question mark with a yellow exclamation point badge on top. Use the **Special Unassign** command to unassign the LUN.

Tip

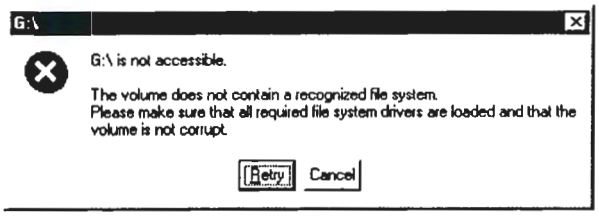
If you need help discovering why a LUN cannot be unassigned, check the system log for possible messages and retry the operation.

The Process Explorer utility from Sysinternals (www.sysinternals.com) can be helpful in determining why a LUN cannot be unassigned. HP is not responsible for any errors that might arise from using this third-party software.

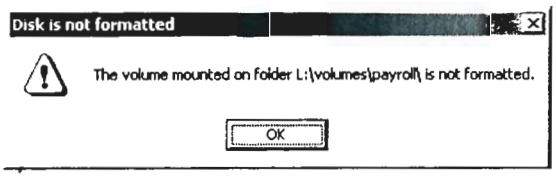
CPMI - CORREIOS
0239
Fls:
3701
Doc:

An assigned disk is not accessible

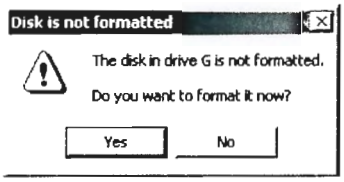
When a LUN is assigned to a Windows host, the volumes on the LUN are listed with drive letters in Windows Explorer or mount points (Windows 2000 only). If a volume is not formatted, one of the following messages appears when you try to access the volume in Windows Explorer.



Windows NT



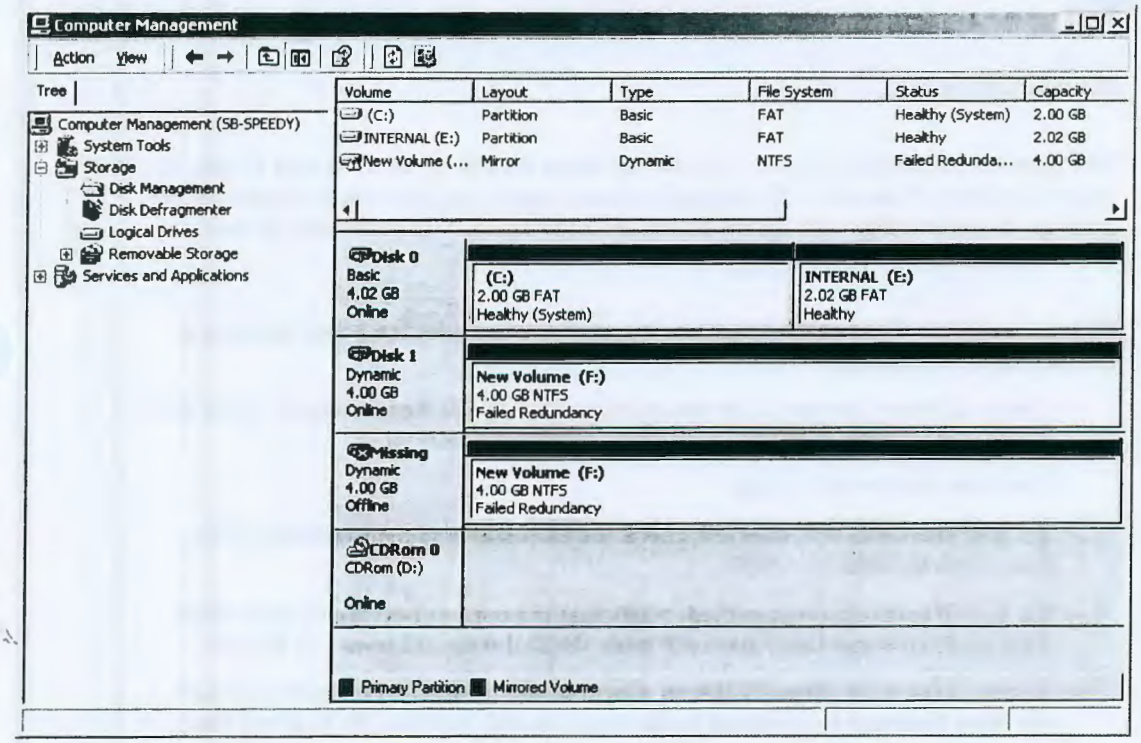
Windows 2000



Windows 2000

Symptom	**Cause**/Solution
One of the dialog boxes shown here appears when you try to access a volume on an assigned LUN.	**The volume is not formatted (does not contain a recognizable file system).** Format the volume. For instructions on formatting volumes in Disk Administrator or Windows 2000 Disk Management, see your Windows documentation.

Dynamic disks are offline (Windows 2000)



Symptom	**Cause**/Solution
When you try to access a dynamic volume on a Windows 2000 host, the volume displays a status of "failed redundancy."	**All of the required disks are not assigned to the host.** Every Fibre Channel LUN that is part of a Windows 2000 dynamic volume should be assigned to an associated LUN group, and the associated LUN group should be assigned to a host.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0240
Fls: 3701
Doc:

The SCSI Adapters control panel lists no LUNs (Windows NT)

Symptom	Cause/Solution
The SCSI Adapters Control Panel does not list any storage network devices.	**The system SCSIPORT driver has not updated its list of devices and LUNs.** To trigger a refresh, close the SCSI Adapters control panel, run Disk Administrator on the host, or use the management server to run the **LUN Discovery** command on the host, and then reopen the control panel.
	There is a Fibre Channel network or storage device problem. The following are possible solutions: – Check all Fibre Channel cable connections. If copper cables are used, check the length and possible earth plane differential potentials. – Check the hub/switch status. – If a RAID is connected, check the LUN status and ensure that there are LUNs created on the RAID. – If a switch is connected, verify that the correct port types are being used. Most RAIDs and HBAs use an F port. JBOD drives and some HBAs use an FL port. – If you are using JBODs on a switch, and devices repeatedly go missing, update the drive firmware to the latest public loop-capable version. JBOD drives have exhibited poor recovery behavior after hot-plugging on a switched network. **Caution** Back up all of your data before updating the drive firmware on the JBOD drives.
	The SCSI Adapters control panel can only list 32 devices per adapter. If an adapter has more attached devices than the control panel can list, the adapter will disappear from the adapters list in the control panel. This does not prevent you from using assigned storage. **Note** This is a Windows NT limitation.

2.718
Irene

hp OpenView storage allocater: HP-UX

Verifying that the daemon is running

To verify that the Storage Allocater daemon is running, type **ps -e | grep TR** and press **Enter**.

If the daemon is running, this command should return the following response:

```
TRAllocater_d
```

For example:

```
sb-c3po# ps -e    |grep TR
 14443 pts/0     0:00 TRAllocater_d
```

If the daemon is not running, check the logfile (**/opt/sanmgr/hostagent/log/lm_daemon.log**) for errors. To start the daemon, type **ioscan** and press **Enter**. If you want to verify that the daemon started successfully, check the logfile.

RQS nº 03/2005 - CN
CPMI - CORREIOS
0241
Fls:
3701
Doc:

An assigned LUN is not accessible to an HP-UX host

Symptom	Cause/Solution
An assigned LUN is not accessible to an HP-UX host.	**The LUN is outside the HP-UX addressing ability. If a device is in peripheral device LUN addressing mode and its LUN is greater than 7, HP-UX hosts will be unable to access the LUN.** If possible, put the device into a different addressing mode, for example, volume set addressing mode. **Note** Some arrays call volume set addressing mode "HP-UX mode." **A hardware addressing conflict exists between devices on a loop.** Set all devices on loops to unique hard address IDs. **The assigned LUN is not on the same storage network segment as the HP-UX host.** Unassign the LUN or move it to the same storage network segment.

2.736

Error during mounting: "not a block device"

Symptom	Cause/Solution
When mounting a device, you get the following error message: `mount: /dev/rdsk/disk_name not a block device`	**There was an error in the mount command. This error occurs when you try to mount a disk using the raw device name rather than the block device name.** Enter the correct command: **mount /dev/dsk/<disk_name> /<mount_point>**

Note Always create HFS/VxFS file systems on "raw" device names and mount file systems on "block" device names; for example:

Raw device name: **/dev/rdsk/device**
Block device name: **/dev/dsk/device**

ROSN° 03/2005 - CN
CPMI - CORREIOS
0242
Fls:
Doc: 3701

A LUN cannot be unassigned from an HP-UX host

Symptom	Cause/Solution
A LUN unassignment fails.	**The LUN contains a mounted file system that is in use.** Stop any processes that are using the file system, and unmount the file system.
	The LUN is configured to be used with storage management software such as LVM or VERITAS Volume Manager. Storage Allocater cannot notify a third-party storage management application that a particular device needs to be removed from its configuration. To unassign a LUN that is being used with third-party storage management software, manually remove it from the control of third-party storage management software.
	The LUN is in use by an application that accesses it directly. Storage Allocater cannot determine which application is using the disk in question, or how to stop the application's access without interrupting what may be a critical process. To unassign this type of LUN, shut down the program that is using the LUN.

Note If you are using HP AutoPath, uninstall AutoPath, unassign the LUN, and then reinstall AutoPath (if desired).

A Storage Data Protector snapshot backup involving an HP-UX hosts fails

Symptom	**Cause**/Solution
A Data Protector snapshot backup failed.	**The hardware paths to unconfigured LUNs (including inactive snapshot LUNs) were not removed before Storage Allocater was activated.** Kill the TRAllocater_d process and restart it by running **ioscan**. Retry the snapshot backup. For information on configuring snapshot backups, see page 152.

ROS Nº 03/2005 - CN
CPMI - CORREIOS
0243
Fls:
3701
Doc:

A rogue host event is displayed for an HP-UX host that is running VERITAS Volume Manager

Symptom	Cause/Solution
The event panel displays the following for an HP-UX host that is running VxVM: `Host <host name> is a rogue server. Detailed messages: 0x100069: A Logical Unit is in use and could not be claimed for filtering.`	**Storage Allocater is unable to filter a LUN that was in use prior to Storage Allocater activation.** Try the following solutions: – Assign the LUN to the host. – If you do not want to assign the LUN to the host, reboot the host.

2712
fls

hp OpenView storage allocater: Solaris

Error during mounting: "not a block device"

Symptom	Cause/Solution
When mounting a device, you get the following error message: `mount: /dev/rdsk/slice_name not a block device.`	**There was an error in the mount command. This error occurs when you try to mount a disk using the raw device name rather than the block device name.** Enter the correct command: **mount /dev/dsk/<slice_name> /<mount_point>**

Note Always create UFS/VxFS file systems on "raw" device names and mount file systems on "block" device names; for example:

Raw device name: **/dev/rdsk/device**
Block device name: **/dev/dsk/device**

205
RQS N° 03/2005 - CN
CPMI - CORREIOS
0244
Fls:
3701
Doc:

A LUN cannot be unassigned from a Solaris host

Symptom	Cause/Solution
A LUN unassignment fails.	**The LUN contains a mounted file system that is in use.** Stop any processes that are using the file system, unmount the LUN, and then unassign it.
	The LUN is configured to be used with third-party storage management software, such as Solstice DiskSuite or VERITAS Volume Manager. Storage Allocater has no way of telling a third-party storage management application that a particular LUN needs to be removed from its configuration. Before unassigning the LUN, manually remove it from the control of third-party storage management software.
	The LUN is in use by an application that accesses it directly. Storage Allocater has no way of knowing what program is using the disk in question, or how to make it stop without interrupting what may be a critical process. Before unassigning this type of LUN, shut down the program that is using it.
	The LUN you are trying to unassign is a tape drive or other nondisk LUN. To unassign a nondisk LUN from a Solaris host, you must use the **Special Unassign** command (page 122).

2710
Irene

An assigned tape library or nondisk device is not available

Symptom	**Cause**/Solution
An assigned nondisk device is not available on a Solaris host.	**The Storage Allocater filter driver does not handle tape devices and other nondisk devices. To use these devices, you must configure the filter driver to allow nondisk devices to be handled by the appropriate drivers when these LUNs are assigned to Solaris hosts.** Use the procedure on page 160 to configure the filter driver.

RG SIN 03/2005 - CN
CPMI - CORREIOS
0245
Fls:
Doc: 101

Assigned LUNs are suddenly unavailable

Symptom	Cause/Solution
Assigned LUNs that were previously available on a Solaris host become inaccessible.	**The HBA driver's configuration utility has replaced Storage Allocater's settings in the /kernel/drv/<driver_name>.conf file (where driver_name is the name of your HBA driver). Open the backup file that you saved during installation and compare the backup file to the current version.** Re-enter any changes that were made when you ran the HBA configuration utility. For more information, see page 159.

2708
fls

A Host with an Emulex HBA reports errors in the /var/adm/messages log

Symptom	**Cause**/Solution
A host with an Emulex HBA reports type 16 errors in the **/var/adm/messages** log.	**The sd_fcst.conf file is configured to search for too many LUNs.** Use one of the following solutions: – Remove some of the targets on the storage network. – Change the **max_luns_per_target** setting to the largest number of LUNs that is configured on any disk array on your storage network. For more information about the max_luns_per_target setting, see the "Activating Storage Allocater" section in the *hp OpenView storage area manager installation guide.*

Note If you try to assign LUNs to a host that is experiencing errors with an Emulex HBA, you may experience problems with the Host Agent software.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0246
Fls:
Doc: 3701

hp OpenView storage allocater: Linux

A LUN cannot be unassigned from a Linux host

Symptom	**Cause**/Solution
The operation fails when you try to unassign a LUN from a Linux host.	**The LUN contains a mounted file system that is in use.** Stop any processes that are using the file system and unmount the file system. Use the **fuser** command to identify the PIDs of processes using the specified files or file systems.
	The LUN is configured to be used with third-party storage management software, and it cannot be unassigned because Storage Allocater cannot remove it from the third-party software's configuration. Manually remove the LUN from the control of third-party storage management software.
	The LUN is in use by an application that accesses it directly. Storage Allocater has no way of knowing what program is using the disk in question, or how to make it stop without interrupting what may be a critical process. Before unassigning this type of LUN, shut down the program that is using it.

2706
Fls:

A Linux host cannot see RUIDs

Symptom	Cause/Solution
When a **cat** operation is performed on /proc/trfilter, no RUIDs are listed.	**There was a problem with the Storage Allocater activation.** To verify this, run the **lsmod** command from the command line. You should see an entry for trfilter with the module usage count. The module usage count must be 2. If the module usage count is not 2, run the command **/opt/sanmgr/hostagent/sbin/trlminstall.sh -uninstall** and then activate Storage Allocater as described in the *hp OpenView storage allocater installation guide.*

SEI 03/2005 - CN
CPMI - CORREIOS
0247
Fls:
3701
Doc:

A Linux host cannot see LUNs

Symptom	**Cause**/Solution
When a **cat** operation is performed on proc/scsi/scsi, no LUNs are listed.	**If Storage Allocater is active on the host, and no LUNs are listed when you perform a cat operation on /proc/scsi/scsi, then the HBA driver is not installed.** Install the appropriate HBA driver. When installing the HBA driver, note the following: 1. The driver object module needs to be present in the **/lib/modules/<kernel_version>/drivers/scsi** directory. 2. To insert the HBA driver, perform an **insmod** operation.

2704

You cannot assign more than 40 LUNs to a Linux host

Symptom	**Cause**/Solution
When 40 LUNs are assigned to a Linux host, additional LUN assignments fail.	**If the value of "Maximum number of SCSI disks that can be loaded as modules" was not set to 128 in the kernel rebuild section of the Linux preinstallation procedure (*hp OpenView storage area manager installation guide*, Chapter 2) and a SCSI driver is loaded as part of the kernel image, you will not be able to assign more than 40 LUNs to the host.** Rebuild the kernel and, under SCSI support, set the "Maximum number of SCSI disks that can be loaded as modules" to 128.

RQS N 03/2005 - CN
CPMI - CORREIOS
0248
Fls:
Doc: 3701

The boot process hangs on a Linux host

Symptom	Cause/Solution
The boot process hangs on a Storage Allocater Linux host.	**Storage Allocater failed to load.** Try the following solutions: 1. **Storage Allocater was installed with a non-SMP kernel, and the system is being restarted with an SMP kernel.** Restart with the kernel on which Storage Allocater was activated. Deactivate Storage Allocater, restart with the SMP kernel, and then activate Storage Allocater. If the boot process hangs after completing this step, continue with step 2. **Note** For instructions on activating and deactivating Storage Allocater, see the *hp OpenView storage area manager installation guide.* 2. **The kernel was recompiled, but the HBA driver was not recompiled to support the new kernel version.** Recompile the HBA driver to support the appropriate kernel version. If the boot process hangs after completing this step, continue with step 3. 3. **Storage Allocater was activated with a kernel that supported 12-byte CDBs, and you are booting with a kernel that has been patched to use 16-byte CDBs.** Restart with the kernel on which Storage Allocater was activated. Enter the command **/opt/sanmgr/hostagent/sbin/trlminstall.sh -postpatch**, and reboot with the 16-byte CDB kernel. For more information about 16-byte CDB support, see page 158.

2702
Paula

hp OpenView storage allocater: AIX

Verifying that the daemon is running

To verify that the Storage Allocater daemon is running, type **ps -e | grep TR** and press **Enter**.

If the daemon is running, this command should return the following response:

```
TRAllocater_d
```

For example:

```
# ps -e |grep TR
14443 pts/0 0:00 TRAllocater_d
```

If the daemon is not running, check the logfile (**/opt/sanmgr/hostagent/log/LM_Daemon.log**) for errors. To start the daemon, enter **/opt/sanmgr/hostagent/sbin/LM_trigger start**. To verify that the daemon started successfully, check the logfile.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0249
Fls:
3701
Doc:

A LUN cannot be unassigned from an AIX host

Symptom	**Cause**/Solution
The operation fails when you try to unassign a LUN.	**The LUN contains a mounted file system that is in use.** Stop any processes that are using the file system, and unmount the file system.
	The LUN is configured to be used with storage management software such as LVM. Storage Allocater cannot notify a third-party storage management application that a particular device needs to be removed from its configuration. To unassign a LUN that is being used with third-party storage management software, manually remove it from the control of third-party storage management software.
	The LUN is in use by an application that accesses it directly. Storage Allocater cannot determine which application is using the disk in question, or how to stop the application's access without interrupting what may be a critical process. To unassign this type of LUN, shut down the program that is using the LUN.

2700
Paula

INDEX

A

accounts
- adding to organizations 48
- closing accounts 51
- removing LUNs from 50
- setup and administration 48

application links
- adding to a device 89
- adding to a device model 92

archiving
- billing data 55
- capacity data 70
- performance data 105

assigning LUNs, Storage Allocater
- assignment rules 121
- assignment types 120
- for dynamic volumes 132
- for HP-UX VERITAS VMSA 129
- for Solaris VERITAS VMSA 129
- for stripe and volume sets (Windows NT) 130
- for volume management software 128
- viewing assigned LUNs (HP-UX) 136

associated LUN groups 118
- using with dynamic volumes 132
- using with dynamic volumes (Windows 2000) 132
- using with FC60 arrays 146
- using with stripe and volume sets (Windows NT) 131
- using with VERITAS VMSA 129

B

bill file name format 57
billing
- basics 42
- getting started 43

billing configuration 52
- billing event triggers 54
- billing export options 53
- billing period 52

billing currency preferences 58
billing data archiving 55
- bill retention period 55
- billing audit retention period 56
- restoring archived bills 57

bills
- integrating with other applications 59

C

capacity
- data archiving 70
- data collection 66
- reports 82

capacity thresholds 76
cfgmgr
- with Storage Allocater 150

charts
- performance
  - Storage Optimizer
    - performance charts 110

221
RQ&N° 03/2005 - CN
CPMI - CORREIOS
0250
Fls:
Doc: 3701

2699
Paula

clustering
Microsoft Cluster Server (Windows NT)
setting up an MSCS share group 127
with Storage Allocater 126
using with Storage Area Manager 34
AIX 36
Windows 2000 34
Windows Clustering (Windows 2000)
setting up a server cluster share group 125
with Storage Allocater 125
collecting capacity data 66
collecting performance data
Storage Optimizer
data collection 103
Command View SDM (Linux)
with Storage Allocater 158
Configuration Status window 124
configuring storage billing 52

D

dead hosts
managing 141
default bridge port 178
device links
adding 13
moving 14
removing 16
device maps
configuring device links 13
adding links 13
moving links 14
removing links 16
layout manager 11
map mode 9
discovery
setting the interval 7
starting 6
stopping 7
Disk Administrator
with Storage Allocater
Windows NT 165
dynamic volumes
with Storage Allocater 132
dynamic volumes (Windows 2000)
importing foreign disks 134
reactivating disks 133
reassigning 132
different host 133
same host 132
unassigning 132
using with associated LUN groups 132

E

events
acknowledging 18
deleting 20
automatic deletion 21
from the event panel 20
exporting 19
filters 23
triggers 25

F

FC60 (HP-UX)
assigning the management LUN 148
guidelines 150
mounting the management LUN 149
with Storage Optimizer 150
FC60 (Windows)
assigning the Universal Xport LUNs 146
guidelines 147–148
HP Universal Xport devices 148
RDAC 145
setting up with Storage Allocater 146
SM60 145
SymArrayCompatibility registry key 146
Universal Xport LUNs 146
with Storage Optimizer 147
FC60 arrays
with Storage Allocater 145–150

2698
Paula

features
Storage Accountant 40
Storage Allocater 116
Storage Area Manager 2
Storage Builder 62
Storage Node Manager 88
Storage Optimizer 98
folders
adding 29
adding members 30
Ftdisk (Windows NT)
special unassignment required 130

G

Getting started with billing 43
groups
associated LUN groups 118
host groups 119
LUN groups 119
share groups 117

H

HBA drivers (Solaris)
configuring 159
host groups 119
host settings, Storage Allocater
modifying host settings (Windows NT hosts) 138
hosts
managing a "dead" host 141
restoring a "dead" host 141
hp OpenView storage area manager bridge
changing the default port 178
configuring for multiple management servers 172
overview 170
user accounts 171
using SSL 174

I

Integrating bills with other applications 59
ioscan
using the ioscan -k command 136
with Storage Allocater 151

L

Linux 16-byte CDBs
with Storage Allocater 158
Linux device files
with Storage Allocater 152
Linux tape LUNs
with Storage Allocater 158
listing
assigned LUNs (HP-UX) 136
logical unit information
modifying 142
viewing 142
LUN groups 119
LUN management
deleting missing LUNs 144
modifying logical unit information 142
viewing logical unit information 142
viewing missing LUNs 144

M

managed directories
Storage Builder
managed directories 72
management server
moving a Storage Allocater host to a new management server 140
maps
configuring device links 13
adding links 13
moving links 14
removing links 16
layout manager 11
map mode 9

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0251
Fls:
3701
Doc:

2697 Paula

metrics, performance
Storage Optimizer
performance metrics 100
Microsoft Cluster Server (Windows NT)
setting up an MSCS share group 127
with Storage Allocater 126
missing logical units
deleting 144
viewing 144
multiple management servers
configuring the Bridge 172

O

Omniback II
with Storage Allocater
Solaris 163
organizational groups
hierarchy 119
host groups 119
LUN groups 119
organizations
adding 31
adding accounts 48
adding members 33
defining properties 32
overview 31

P

performance
baselines and automatic thresholds 107
charts 110
data archiving 105
data collection 103
metrics 100
Performance Monitor
with Storage Allocater
Windows NT 166
Physical and logical space 64

R

registry settings (Windows NT)
ExtendedLogging 139
LargeLuns 168
LunRescan 167
ScanDisconnectedDevices 167
SymArrayCompatibility 139
removing LUNs from accounts 50
reports
capacity 82
RUID-based device files (Linux) 153

S

SCSIPORT (Windows NT)
optimizing with Storage Allocater
LargeLuns registry setting 168
LunRescan registry setting 167
ScanDisconnectedDevices registry
setting 167
SecurePath
with Storage Allocater
Solaris 164
security groups
associated LUN groups 117
share groups 117
service levels
creating 45
deleting service levels 47
setting LUN service levels 45
setup and administration 45–47
setting up accounts 48
setting up service levels 45
share groups 117
setting up a server cluster share group 125
setting up an MSCS share group 127
using with clustering 125
using with FC60 arrays 146
Solaris 163
Solaris HBAs
with Storage Allocater 159

2696
Paula

special unassign
Configuration Status window 124
HP-UX hosts 122
required reboot 122
rules for special unassignments 122
SSL 174
status summary, viewing 95
Storage Accountant
accounts 48–51
billing basics 42
billing configuration 52–54
features 40
getting started with billing 43
service levels 45–47
setting currency preferences 58
troubleshooting 180–185
Storage Allocater
Activation wizard
with clustering 125, 127
with dynamic volumes 132
with FC60 arrays 147, 148
with stripe and volume sets 130
with VMSA 129
with volume management software 128
with volume sets 128
features 116
groups
associated LUN groups 118
host groups 119
LUN groups 119
share groups 117
interoperability 145–168
HP-UX ioscan 151
with AIX cfgmgr 150
with Command View SDM (Linux) 158
with Disk Administrator (Windows NT) 165
with FC60 arrays 145
with Linux 16-byte CDBs 158
with Linux device files 152
with Linux tape LUNs 158
with Omniback II, Storage Data Protector, and Solaris tape libraries 163
with Performance Monitor (Windows NT) 166
with SCSIPORT (Windows NT) 167
with SecurePath (Solaris) 164
with Solaris HBAs 159
with Solaris tape and nondisk devices 160
with Storage Data Protector 152
with StorageWorks virtual arrays 152
managing assignments 120–137
managing hosts 138–141
managing LUNs 142–144
troubleshooting 191–220
Storage Area Manager
cluster environments 34
device maps 9
discovery 6
events 17
features 2
folders 29
maps 9
organizations 31
users 4
Storage Builder
capacity thresholds 76
data archiving 70
data collection 66
features 62
physical and logical space 64
reports 82
troubleshooting 186–188
Storage Data Protector
with Storage Allocater
HP-UX 152
Solaris 163
Storage Node Manager
application links 89
features 88
status summary 95

RQS nº 03/2005 - CN
CPMI - CORREIOS
0252
Fls: 3701
Doc:

2695 Paula

Storage Optimizer
baselines and automatic thresholds 107
data archiving 105
features 98
troubleshooting 189–190
StorageWorks virtual arrays
with Storage Allocater 152
stripe and volume sets (Windows NT)
using with Storage Allocater 131

T

tape and nondisk devices
with Storage Allocater
Solaris 160
tape libraries
with Storage Allocater
Solaris 163
thresholds
capacity 76
performance 107

U

unassigning LUNs, Storage Allocater
special unassignments 122
user accounts 171
users, adding 4

V

VERITAS VMSA
with Storage Allocater 129
volume management software
with Storage Allocater 128

W

windows
Configuration Status 124

2694
Paula

Copyright © 2002
Hewlett-Packard Company
Printed in U.S.A.
J5364-90002

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0253
Fls: 3701
Doc:

Apêndice AF

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 0254
3701
Doc:

2693 Paula

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.

ROS Nº 03/2005 - CN
CPMI - CORREIOS
IPC-353
0255
Fls: 3701
Doc:

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

2691
Paula

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.

ROG NF 03/2005 - CN -
CPMI - IPC-355 - DS
0256
Fls: 3701
Doc:

2690
Paula

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,

2689
Paula

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:

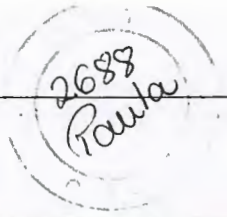
Command	Purpose
`Router(config)# route-map map-tag [permit | deny] [sequence-number]`	Defines any route maps needed to control redistribution.

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.

POS Nº 03/2005 - CN
CPMI - IPC-357
0257
Fls: 3701
Doc:



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.

2687 Paula

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
ep 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.

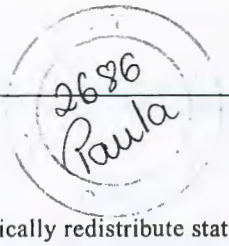
The metrics of one routing protocol do not necessarily translate into the metrics of another. For example, the RIP metric is a hop count and the IGRP metric is a combination of five quantities. In such situations, an artificial metric is assigned to the redistributed route. Because of this unavoidable 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.

IPC-355
CPML - CORREIOS
0258
Fls: 3701
Doc:



- 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.

2685
Paula

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.

ROSN nº 03/2005 - CN
CDMA CORREIOS
IPC-361
0259
Fls:
Doc: 3701

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.

2683
Paula

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.

IPC-363
CPMI - CORREIOS
0260
Fls:
Doc: 370011

2682
Paula

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.

2681 Paula

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:

IPC-365
CPMI - CORREIOS
0261
Fls:
3701
Doc:

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.

2679
Paula

- 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
`uter(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.

CPMI - CORREIOS
IPC-367
0262
Fls:
3701
Doc:

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.

2677
Paula

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.

RQS Nº 03/2005 - CN
IPC-369
0263
Fls:
3701
37

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.

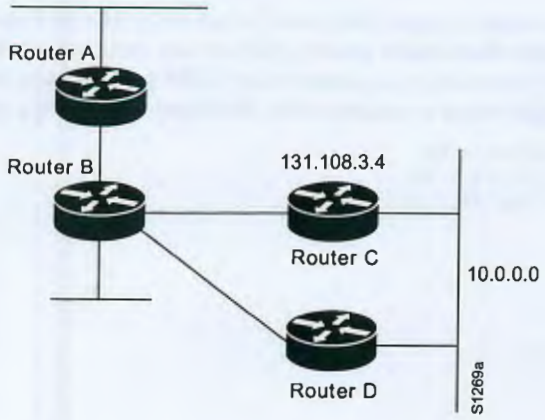
```
interface ethernet 0
 ip address 131.107.1.1 255.255.255.0
! 8 bits of host address space reserved for ethernets

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
```

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
```

2673
Paula

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
```

IP and EIGRP Redistribution Examples

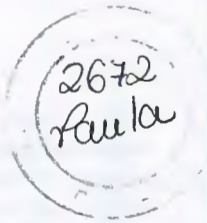
This section provides a simple RIP redistribution example and a complex redistribution example between Enhanced IGRP (EIGRP) and BGP.

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:

IPC-373
CPMI CORREIOS
Fls: 0265
Doc: 3701




```
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.

2671
Paula

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
!
```


DOC Nº 03/2005 - CN
CPMI - IPC-375
0266
Fls:
3701
Doc:

2670
Pauba

```
! 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.

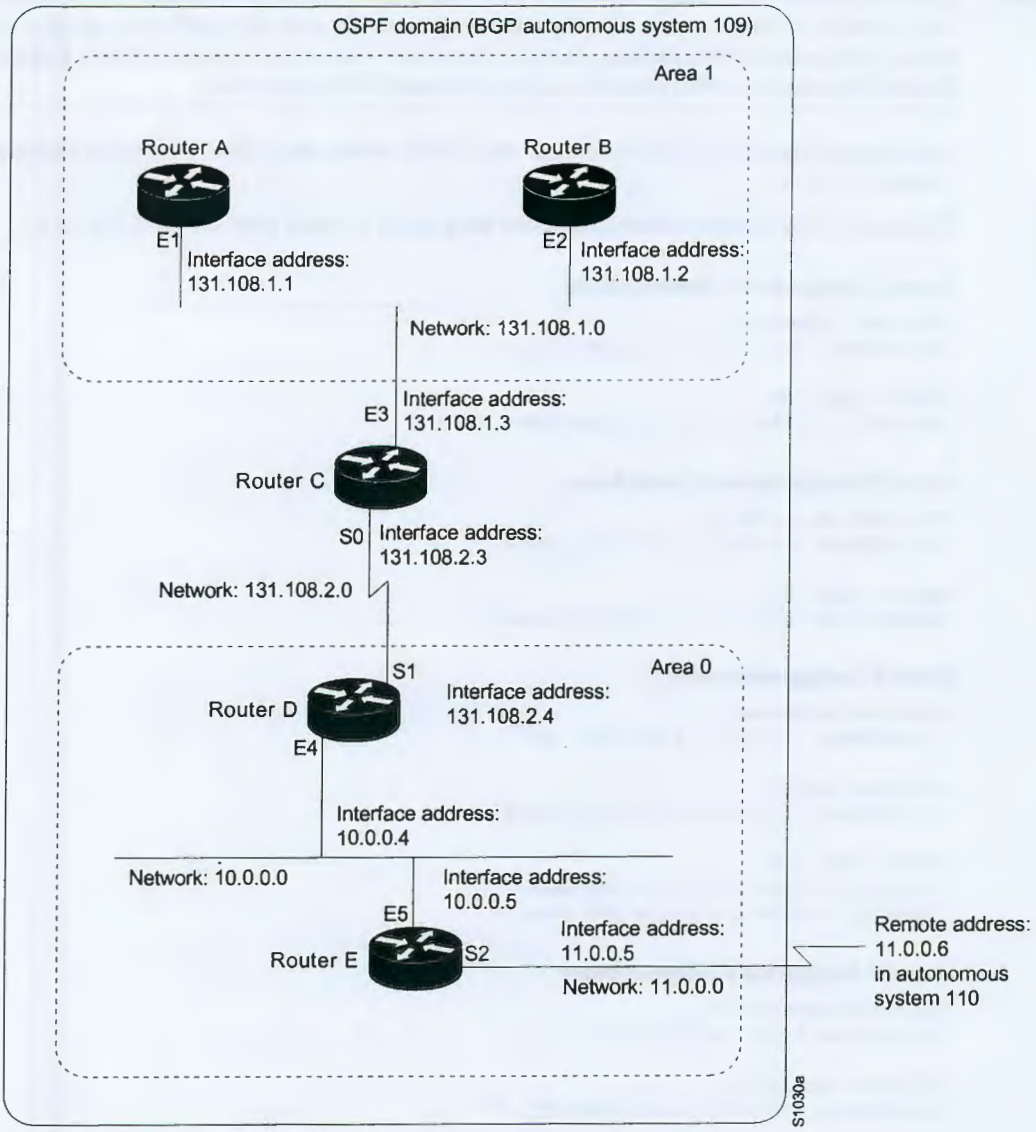
This process of attaching interfaces to OSPF areas continues for all **network** commands. Note that the last **network** command in this example is a special case. With this command, all available interfaces (not explicitly attached to another area) are attached to Area 0.

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.

2669
Paula

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.

IPC-377
CPMI - CORREIOS
0267
Fls:
Doc: 3701

2668
Paula

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
```

2667
Paula

```
router bgp 109
 network 131.108.0.0
 network 10.0.0.0
 neighbor 11.0.0.6 remote-as 110
```

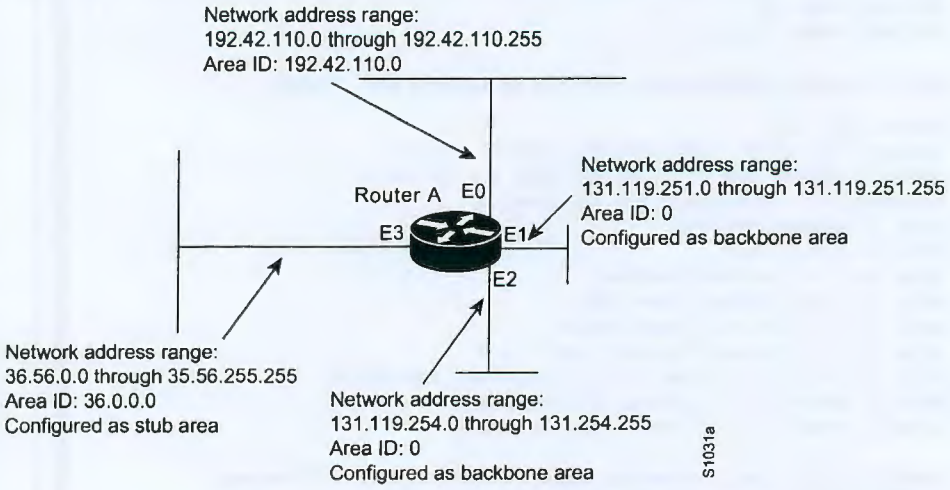
Complex OSPF Configuration Example

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:

RJS Nº 03/2005 - CN
CPMI - IPC-279
Fls: 0268
3701
Doc:

```
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
```

2665
Paula

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
```


03/2005 - CN
CPMI - IPC-381
0269
Fls:
Doc:
3701

2664
Paula

```
 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.

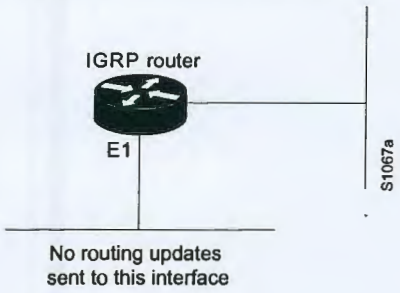
2663
Paula

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.

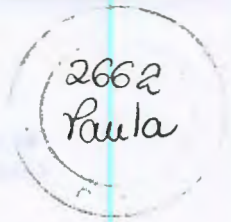
The **passive-interface** router configuration command typically is used when the wildcard specification on the **network** router configuration command configures more interfaces than is desirable. The following configuration causes OSPF to run on all subnets of 131.108.0.0:

```
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
```


CPMI - CORREIOS
IPC-383
0270
Fls:
Doc: 3701




```
 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
```

2661
Fls

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
```


CPMI - IPC-385
Fls: 0271
Doc: 3701

2660
Paul

```
 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
```

Apêndice AG

ROS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 0272
Doc: 3791

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

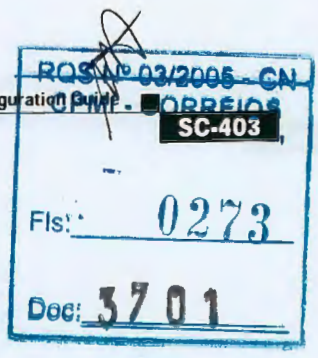
This chapter includes the following sections:

- 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

rotecting 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



2658 Paula

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 commands 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.

2654
Paula

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.

SC-405
CPMI CORREIOS
0274
Fls:
3701
Doc:

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.

2655
Paula

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.

DOC Nº 03/2005 - CN
CPI SC-407 EIOS
0275
Fls:
3701
Doc:

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.

2653
Paula

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.

SC-409
CORREIOS
0276
Fls:
Doc: 3701

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

2651
Paula

- 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>
```


SC-411
CPMI - CORREIOS
0277
Fls:
3701
Doc:

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.

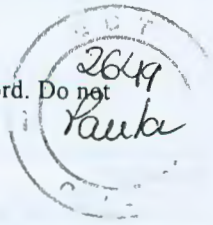
Step 2 Enter **Yes** when asked if you want to set the manufacturers' addresses.

The following prompt appears:

```
TEST-SYSTEM >
```

Step 3 Enter **enable** to enter enable mode:

```
TEST-SYSTEM > enable
```



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.

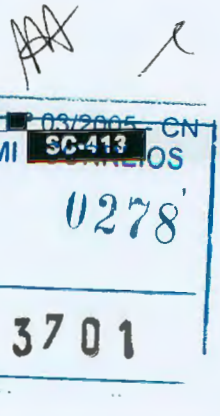
See the hardware installation and maintenance publication for your product for specific information about configuring the processor configuration register for factory diagnostic mode. Table 27 summarizes the hardware or software settings required by the various products to set factory diagnostic mode.

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.

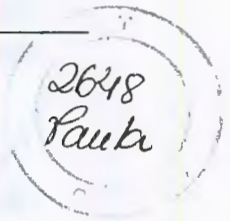
Configuring Identification Support

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 sets 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

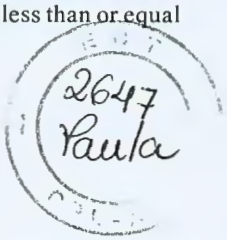
In the following example, you define an enable password for privilege level 10 for system operators and make **clear** and **debug** commands available to anyone with that privilege level enabled.

```
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:

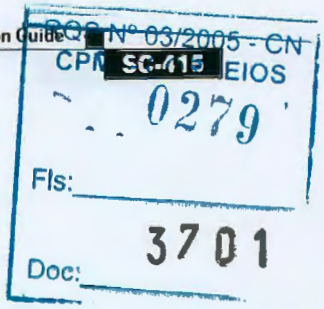
```
username B password b-c_secret
```

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
```

Apêndice AH

RQS Nº 03/2005 - CP
CPMI - CORREIOS
Fls: 0280
Doc: 3701

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:

- Voice Port Configuration Overview, page 38
- Analog Voice Ports Configuration Task List, page 42
- Configuring Digital Voice Ports, page 56
- 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

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.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
VC-37
0281
Fls:
3701
Doc:

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

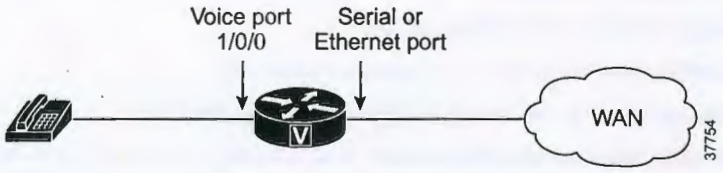


Figure 11 Telephone to PSTN

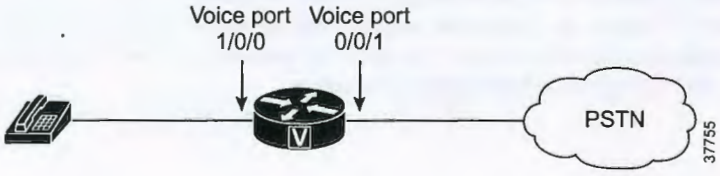


Figure 12 PBX-to-PBX over a WAN

2643
Paula

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.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
VC-39
Fls:
Doc: 3701

Figure 13 FXS Signaling Interfaces

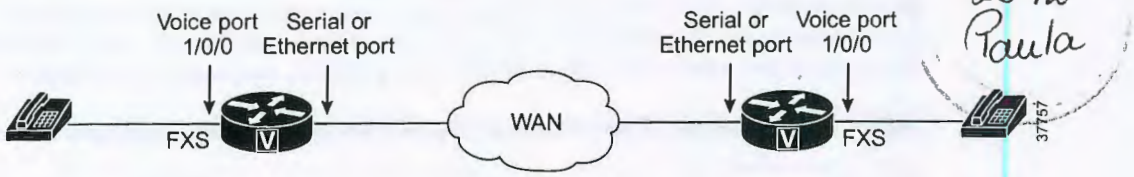


Figure 14 FXS and FXO Signaling Interfaces

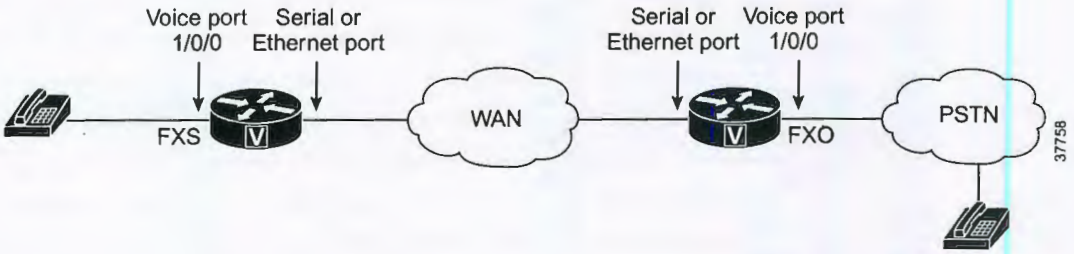
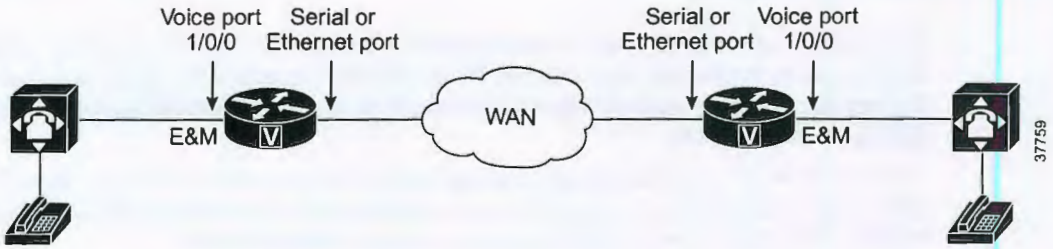


Figure 15 E&M Signaling Interfaces



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.

2641 Paula

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.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
VC-41
0283
Fls:
3701
Doc:

2640
Paula

PBXs 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

2639
Fls.

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.

RQS Nº 03/2005 - CN
CPMI
VC-43
0284
Fls:
3701
Doc:

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

2637
Paula

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*.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
VC-45
0285
Fls:
Doc: 3701

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 channels 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.

2635
Paula

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.

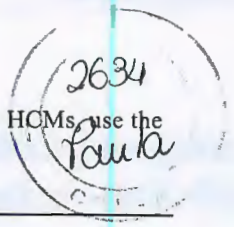
Codec complexity is either medium or high. The difference between medium- and high-complexity codecs is the amount of CPU power necessary to process the algorithm and, therefore, the number of voice channels that can be supported by a single DSP. All medium-complexity codecs can also be run in high-complexity 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.

RQS Nº 03/2005 - CN
COMI - CORREIOS
VC-47
0286
Fls:
Doc: 3701



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.

2633
Paula

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.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
VC-49
0287
Fls:
Doc:
3701

	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.

2631
Paula

	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.

ROS Nº 03/2005 - CN
CPMI - CORREIOS
VC-51
0288
Fls:
3701
Doc:

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:

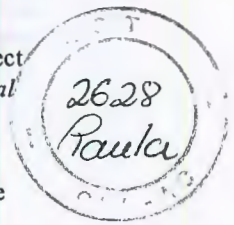
	Command	Purpose
Step 1	`Router(config)# pots country` *country*	Specifies the country to use for country-specific default settings for physical characteristics. Enter **pots country ?** for a list of supported countries and the codes to enter. A default country is not defined.
Step 2	`Router(config)# 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.

ECT 2629 Paula

	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.
ep 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.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0289
Fls:
Doc: 3701

	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,
```

2627
Paula

```
  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
```


RQS Nº 03/2005 - CN
CPMI - CORREIOS
VC-55
0290
Fls:
Doc: 3701

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 lines 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 support 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

2625
Paula

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

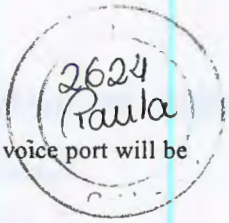
  The memory required for high-volume applications may be greater than that listed. Support for digital T1 packet voice trunk network modules is included in Plus feature sets. The IP Plus feature set requires 8 MB of Flash memory; other Plus feature sets require 16 MB.
- (Cisco 2600 and 3600 series routers) 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.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
VC-57
Fls: 0291
Doc: 3701

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

2623
Paula

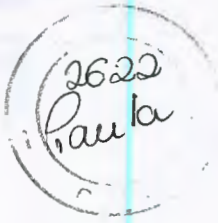
Table 8 Digital Voice Slot/Port Designations (continued)

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

RQS Nº 03/2005 - CN
CPMI CORREIOS
VC-59
Fls: 0292
Doc: 3701

The following is **show voice port summary** sample output for 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
```



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.

2621
Paula

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

RQS Nº 03/2005 - CN - CPMI - CORREIOS
VC-61
Fls: 0293
Doc: 3701

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.

2619
Pauba

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.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
VC-63
0294
Fls:
3701
Doc:

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.

2617
Fls:

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.

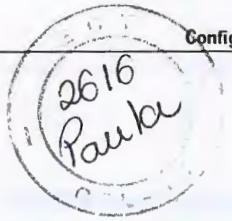
Note On Cisco 2600 and 3600 series routers with digital T1/E1 packet voice trunk network modules, codec complexity cannot be configured if DS0 groups are configured. Use the **no ds0-group** command to remove DS0 groups before configuring codec complexity.

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.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
VC-65
0295
Fls:
3701
Doc:



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.

2615
Fax/Modem

	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

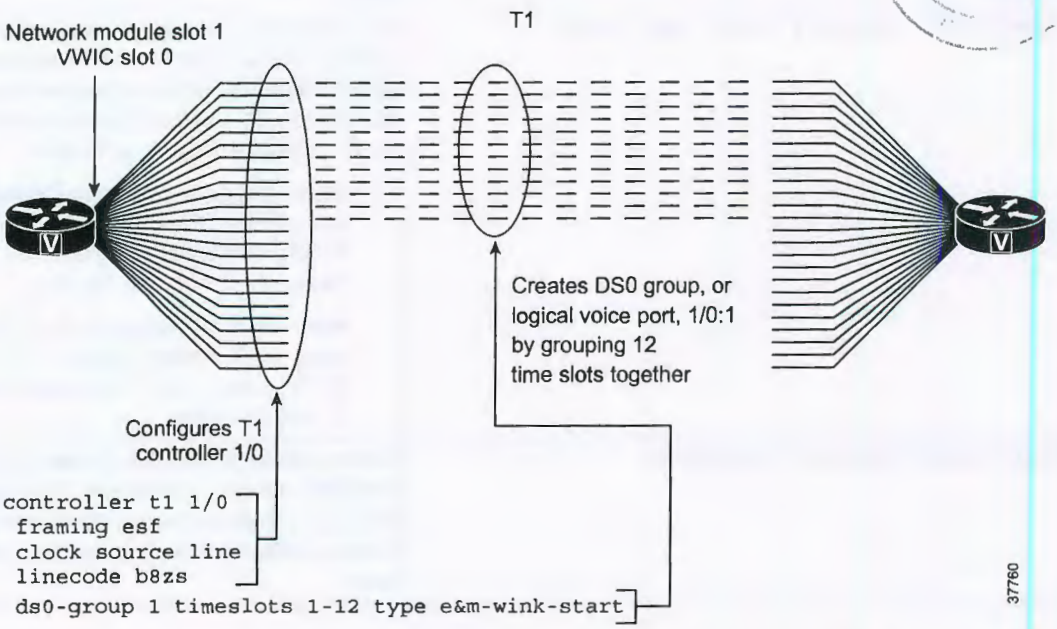
The purpose of configuring controllers for digital T1/E1 voice ports is to match the configuration of the router to the line characteristics of the telephony network connection being made so that voice and signaling can be transferred between them and so that logical voice ports, or DS0 groups, may be 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.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
VC-67
0296
Fls:
Doc: 3701

Figure 16 T1 Controller Configuration on Cisco 2600 or 3600 Series Routers



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.

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:

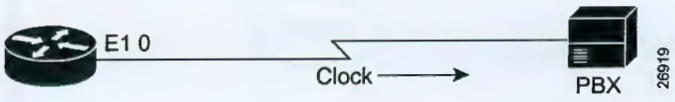
- When both ports are set to line clocking with no primary specification, port 0 is the default primary clock source and port 1 is the default secondary clock source.
- When both ports are set to line and one port is set as the primary clock source, the other port is by default the backup or secondary 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:

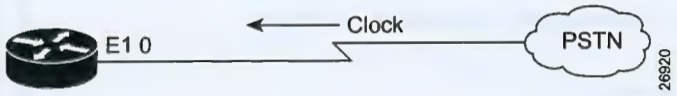
```
controller E1 1/0
 framing crc4
 linecoding hdb3
 clock source internal
 ds0-group timeslots 1-15 type e&m-wink-start
```

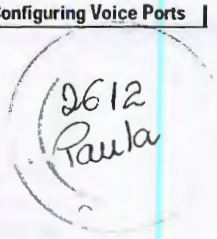
Figure 17 Single Voice Port Providing Clocking



- 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





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.

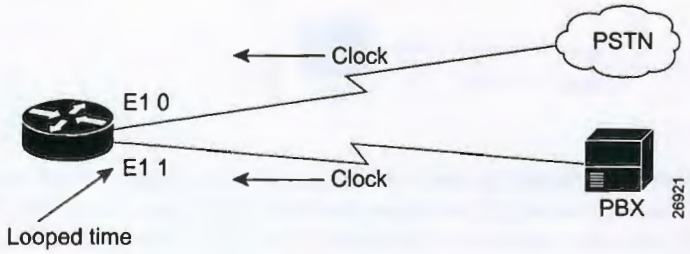
  Before looking at the details, consider the following as they pertain to the clocking method:

  - 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:

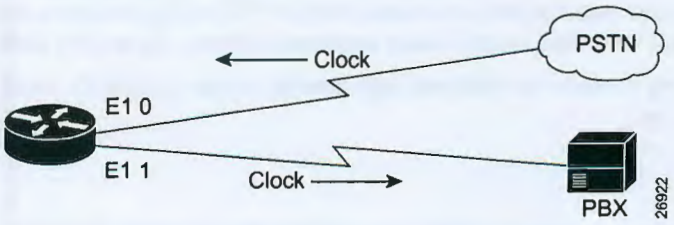
```
controller E1 1/0 << description - connected to the CO
 framing crc4
 linecoding hdb3
 clock source line primary
 ds0-group timeslots 1-15 type e&m-wink-start
!
```

```
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

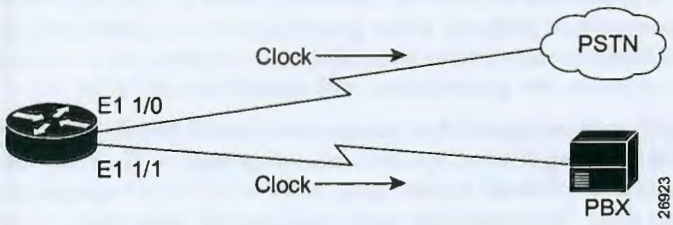


The following configuration sets up this clocking method:

```
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.

2609
Paula

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.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0299
Fls:
3701
Doc:

3701

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**.

2607 Paula

	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**.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0300
Fls:
Doc: 3701

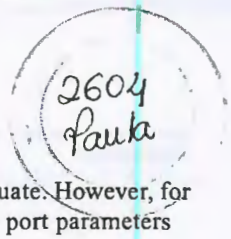
2606 Paula

	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.

2605
Paula

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.

REQ Nº 03/2005 - CN
CPMI - CORREIOS
0301
Fls:
Doc: 3701



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.

2603
Paula

	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.

ECT-2005 - CN
CPMI - CORREIOS
0302
Fls:
3701
Doc:

	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.

2601 Paula

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:

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0303
Fls:
3701
Doc:

	Command	Purpose
Step 1	`Router(config-voiceport)# condition {tx-a-bit | tx-b-bit | tx-c-bit | tx-d-bit} {rx-a-bit | rx-b-bit | rx-c-bit | rx-d-bit} {on | off | invert}`	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).
		The keywords are as follows: • **on**—Sets the bit to 1 permanently. • **off**—Sets the bit to 0 permanently. • **invert**—Changes the state to the opposite of the original transmit or receive state. **Note** The **show voice port** command reports at the protocol level, and the **show controller** command reports at the driver level. The driver is not notified of any bit manipulation using the **condition** command. As a result, the **show controller** command output does not account for the bit conditioning.
Step 2	`Router(config-voiceport)# define {tx-bits | rx-bits} {seize | idle} {0000 | 0001 | 0010 | 0011 | 0100 | 0101 | 0110 | 0111 | 1000 | 1001 | 1010 | 1011 | 1100 | 1101 | 1110 | 1111}`	(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 **define** 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: • **tx-bits**—Indicates the pattern applies to transmit signaling bits.

2599
Paula

	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:

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0304
Fls:
Doc:
3701

	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.

2597
Paula

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.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0305
Fls:
Doc: 3701

2596 Paula

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.

2595
Paula

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**.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0306
Fls:
Doc: 3701

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` *dBmO*	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` *dBmO*	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` *dBmO*	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).

2593
Paula

	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:

RQS Nº 03/2005 - CN
CPMI CORREIOS
0307
Fls:
3701
Due:

	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 a busy tone, reorder tone, or an out-of-service tone 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.

2591
Paula

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.
ep 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.

ROS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 0308
3701
Doc.
VC-91

	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.

2589
Paula

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.

ECT/ECOS N° 03/2005 - CN
CPMI - CORREIOS
0309
Fls:
Doc: 3701

2588 Paula

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.

2587
Paula

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**.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 0310
Doc: 3701

	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:

2585
Paula

	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.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0311
Fls:
Doc: 3701

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*}

2583
RQS Nº 03/2005 - CN
CPMI - CORREIOS
0312
Doc: 3701

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
```

2581 Paula

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0313
Fls:
3701
Doc:

```
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
```

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
```

2577
Paula

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.
```

ROS Nº 03/2005 - CN
CPMI - CORREIOS
0315
Fls:
3701
Doc:

```
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
```

2576 Paula

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
```

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
```

2575 fls 0316
RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 0316
Doc: 3701

```
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
```

2573
Paula

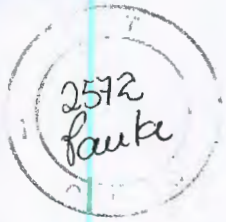
```
PeerIfIndex=35
LogicalIfIndex=0
DisconnectCause=10

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
```

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0317
Fls:
3701
Doc:

Troubleshooting Analog and Digital Voice Port Configurations

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.

2571 Paula

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.)

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0318
Fls:
3701
Doc:

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:

- 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

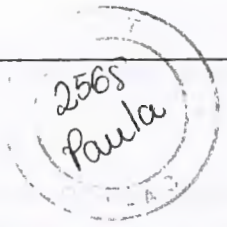
Step 1	**Cisco 2600 and 3600 Series Routers Analog Voice Ports**
	`Router# test voice port slot/subunit/port detector {m-lead | battery-reversal | loop-current | ring | tip-ground | ring-ground | ring-trip} {on | off}`
	
	Cisco 2600 and 3600 Series Routers Digital Voice Ports
	`Router# test voice port 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.

2569 Paula

	Command	Purpose
	Cisco MC3810 Multiservice Concentrators Digital Voice Ports `Router# test voice port slot:ds0-group detector {m-lead | battery-reversal | loop-current | ring | tip-ground | ring-ground | ring-trip} {on | off}`	

Step 2	**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} disable`
	
	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} disable`
	
	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} disable`
	
	Cisco MC3810 Multiservice Concentrators Digital Voice Ports
	`Router# test voice port slot:ds0-group detector {m-lead | battery-reversal | loop-current | ring | tip-ground | ring-ground | ring-trip} disable`
		Identifies the voice port on which you want to end the test. Enter a keyword for the detector 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 detector is in the forced state.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0319
Fls:
Doc: 3701



Loopback Function Tests

To establish loopbacks 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 loopback {local | network}`
	
	Cisco 2600 and 3600 Series Routers Digital Voice Ports
	`Router# test voice port slot/port:ds0-group loopback {local | network}`
	
	Cisco MC3810 Multiservice Concentrators Analog Voice Ports
	`Router# test voice port slot/port detector loopback {local | network}`
	
	Cisco MC3810 Multiservice Concentrators Digital Voice Ports
	`Router# test voice port slot:ds0-group loopback {local | network}`
		Identifies the voice port you want to test and enters a keyword for the loopback direction.
		
		Note A call must be established on the voice port under test.

Step 2	**Cisco 2600 and 3600 Series Routers Analog Voice Ports**
	`Router# test voice port slot/subunit/port loopback disable`
	
	Cisco 2600 and 3600 Series Routers Digital Voice Ports
	`Router# test voice port slot/port:ds0-group loopback disable`
	
	Cisco MC3810 Multiservice Concentrators Analog Voice Ports
	`Router# test voice port slot/port detector loopback disable`
	
	Cisco MC3810 Multiservice Concentrators Digital Voice Ports
	`Router# test voice port slot:ds0-group loopback disable`
		Identifies the voice port on which you want to end the test and enters the keyword disable to end the loopback.

2567
Paula

Tone Injection Tests

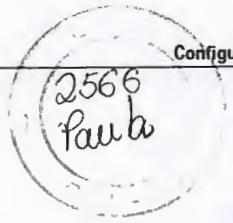
To inject a test tone into a voice port, use the following commands in privileged EXEC mode:

	Command	Purpose

Step 1	**Cisco 2600 and 3600 Series Routers Analog Voice Ports**
	`Router# test voice port slot/subunit/port inject-tone {local | network} {1000hz | 2000hz | 200hz | 3000hz | 300hz | 3200hz | 3400hz | 500hz | quiet}`
	Cisco 2600 and 3600 Series Routers Digital Voice Ports
	`Router# test voice port slot/port:ds0-group inject-tone {local | network} {1000hz | 2000hz | 200hz | 3000hz | 300hz | 3200hz | 3400hz | 500hz | quiet}`
	Cisco MC3810 Multiservice Concentrators Analog Voice Ports
	`Router# test voice port slot/port detector inject-tone {local | network} {1000hz | 2000hz | 200hz | 3000hz | 300hz | 3200hz | 3400hz | 500hz | quiet}`
	Cisco MC3810 Multiservice Concentrators Digital Voice Ports
	`Router# test voice port slot:ds0-group inject-tone {local | network} {1000hz | 2000hz | 200hz | 3000hz | 300hz | 3200hz | 3400hz | 500hz | quiet}`
		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.
		Note A call must be established on the voice port under test.

Step 2	**Cisco 2600 and 3600 Series Routers Analog Voice Ports**
	`Router# test voice port slot/subunit/port inject-tone disable`
	Cisco 2600 and 3600 Series Routers Digital Voice Ports
	`Router# test voice port slot/port:ds0-group inject-tone disable`
	Cisco MC3810 Multiservice Concentrators Analog Voice Ports
	`Router# test voice port slot/port detector inject-tone disable`
	Cisco MC3810 Multiservice Concentrators Digital Voice Ports
	`Router# test voice port slot:ds0-group inject-tone disable`
		Identifies the voice port on which you want to end the test and enter the keyword **disable** to end the test tone.
		Note The **disable** keyword is available only if a test condition is already activated.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0320
Fls:
Doc: 3701
VC-115



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.

2565
Paula

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.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0321
Fls:
Doc: 3701

2564
Paula

Cisco Systems

Data Sheet

CiscoWorks **Campus Manager**

Campus Manager is a key component in the CiscoWorks family of management solutions designed to make Cisco networks the most manageable and available in the industry. Today's networks are critical business assets, and require sophisticated tools for administering, monitoring and configuring Layer 2 services. Designed for enterprise network operations staff, Campus Manager provides powerful tools with built-in network intelligence to reduce the complexity and automate manual tasks associated with maintaining complex physical and logical network infrastructures.

Campus Manager Overview

Campus networks are at the heart of business and mission-critical systems. The requirement to understand, monitor, and react to changing networking conditions drives the need for sophisticated, yet easy-to-use management tools. Campus Manager is part of the LAN Management Solution, part of the broad range of CiscoWorks network management solutions.

New in Version 3.3:

In addition to the rich set of management features already included, the new version of Campus Manager has been enhanced to provide even greater manageability for Cisco networks. New benefits include:

- Improved application performance
- Doubled capacity for tracking end users

Key Campus Manager features include:

- Intelligent discovery and display of Layer 2 networks on browser-accessible topology maps, independent of VTP server
- Configuration of virtual LAN (VLAN)/ LAN Emulation (LANE) and asynchronous transfer mode (ATM) services and assignment of switch ports to those services
- Link and device status display based upon Simple Network Management Protocol (SNMP) polling
- Identification of Layer 2 configuration discrepancies
- Diagnostic tools for connectivity related problems between end stations, and Layer 2 and Layer 3 devices
- Automatic location and correlation of information on users by media access control (MAC), IP address, NT or NetWare Directory Services (NDS) login or UNIX host name, with their physical connections to the switched network
- Visibility and launch point of Cisco CallManager from topology services as well as tracking of phone handset to IP, Mac address, and switch port
- Layer 2 and Layer 3 path trace between source and destination handsets
- Export of topology maps to Visio
- Java plugins to improve graphical user interface (GUI) performance

REG Nº 03/2005 - CN
CPMI - CORREIOS
0322
Fls:
3701
Doc:

Cisco Systems, Inc.
All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement

- Ability to form Custom Groups in Topology View based on criteria like SysLocation, SysName and IP address/ Subnet mask.
- Secure communication between the client browser and Campus applications using Secure Socket Layer (SSL) protocol.

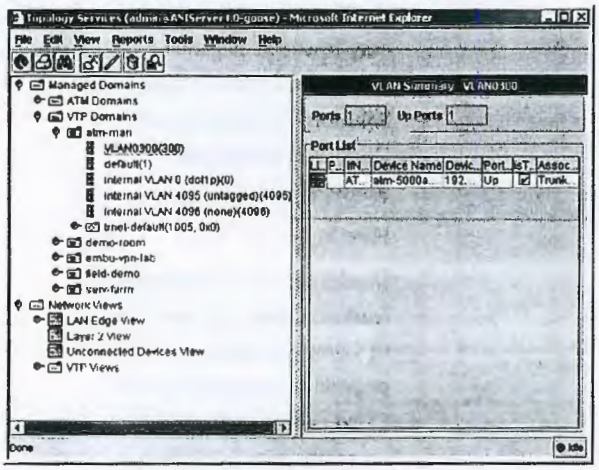
Campus Manager enables administrators to more easily change, monitor, and control network relationships, making them more effective in delivering business-critical and advanced networking services to their users and customers.

Campus Manager is a suite of applications launched from a common "management desktop" used by all Web-based CiscoWorks applications. Campus Manager contains three applications that can be launched from the client's browser:

- Topology Services—This is the principal interface to a variety of large scale topology maps, tabular summaries, reports, and configuration services of the Layer 2 network. A directory-like tree interface lists physical Layer 2 and logical, Virtual Trunking Protocol (VTP), and ATM domain views along with table summaries of the devices and interface associated with these views. This tree structure acts as the launching point for topology maps, discrepancy reporting functions, and configuration services. The integrated VLAN and LANE configuration capabilities, ATM soft permanent virtual circuit (PVC) configuration and diagnostic tools, along with physical and logical configuration discrepancy checking reports and highlighting tools are found within the Topology Services menus. It also supports discovery and display of Cisco Customer Response Applications, and reports on services of these devices.

  Ability to form custom groups based on dynamic and static rules for the group membership. System defined groups and user defined grouping can be created by network administrators and users respectively and allows grouping by developing rules based on criteria such as IP address, subnets, SysLocation, SysName, SysContact, Image Version and hostname. A rules editor allows for creating, editing Topology groups and defines rules for membership.

Figure 1
Topology Services Tabular View



All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

2562
Paula

Figure 2
VTP Domain Topology Map

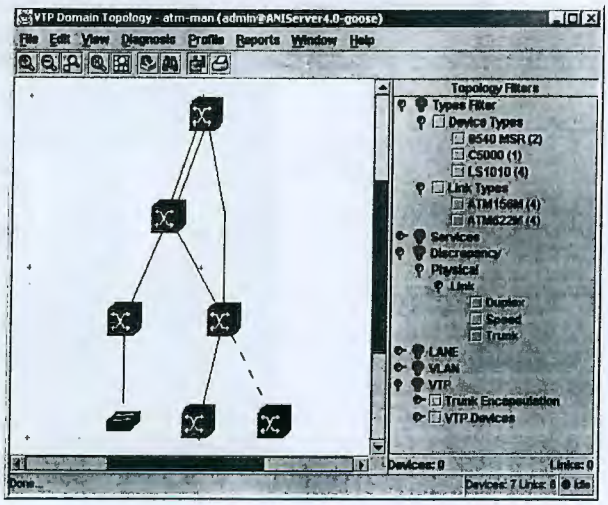
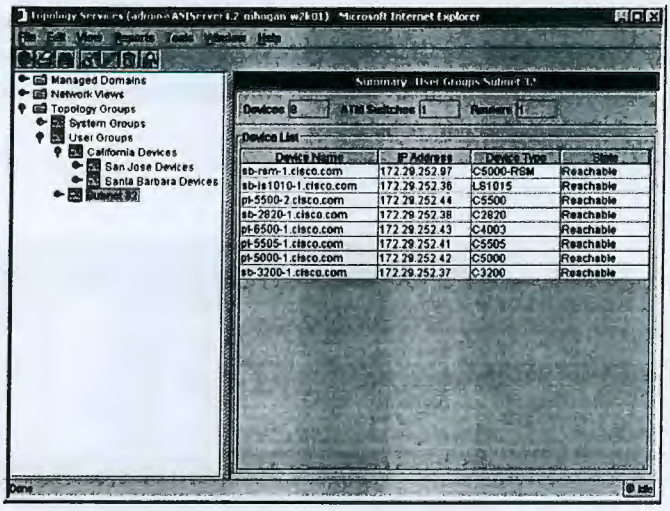


Figure 3
Forming Topology Groups

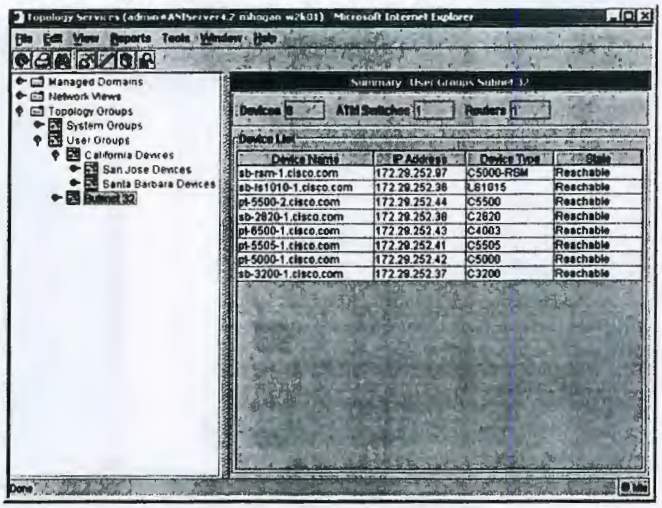


RQS Nº 03/2005 - CN
CPMI - CORREIOS
0323
Fls:
Doc: 3701

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

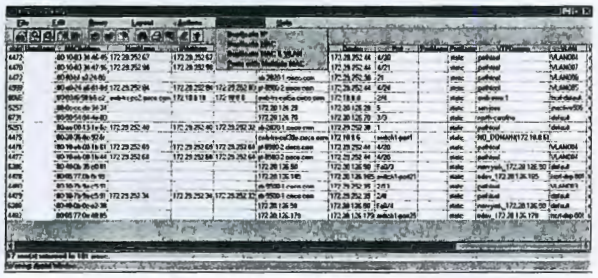
2561
Pub

Figure 4
Topology Group in Topology Maps



- User Tracking—Designed to assist in locating end-station connections at the access switch, this application is a useful tool in troubleshooting or connectivity analysis. Through automated acquisition, a table of end-user stations and Layer 2 connection information is constructed. This table can be sorted and queried allowing administrators to easily find users. Users can be identified by name, IP handset, MAC and IP address, as well as the switch port and switch that they are connected, along with VLAN and VTP assignment of the port. Predefined reports, such as duplicate MAC per switch port, or duplicate IP addresses, enable managers to locate mobile users or violations in port policies.

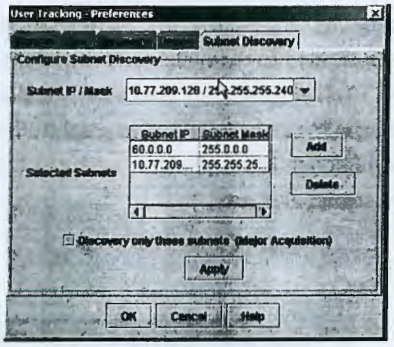
Figure 5
User Tracking



Cisco Systems, Inc.
All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

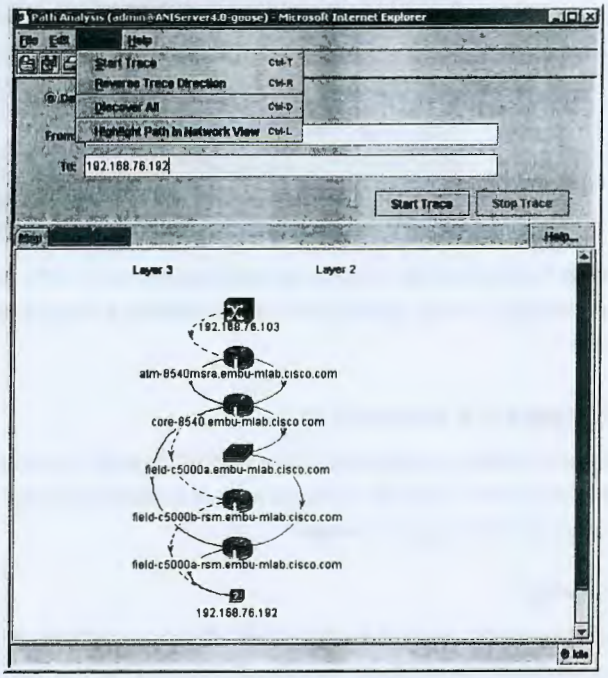
2560
Paula

Figure 6
Subnet based acquisition



- Path Analysis—An application for switched network management, this is an extremely powerful tool for connectivity troubleshooting. Path Analysis utilizes User Tracking, topology services, and real-time spanning tree information to determine Layer 2 and Layer 3 connectivity between two end-points, or IP Handsets, in the network. The resulting trace is presented in graphical topology views that illustrate the Layer 2 and Layer 3 devices, path direction and link types, and in tabular formats that provide specific interface, IP address, VLAN, and link type information.

Figure 7
Path Analysis



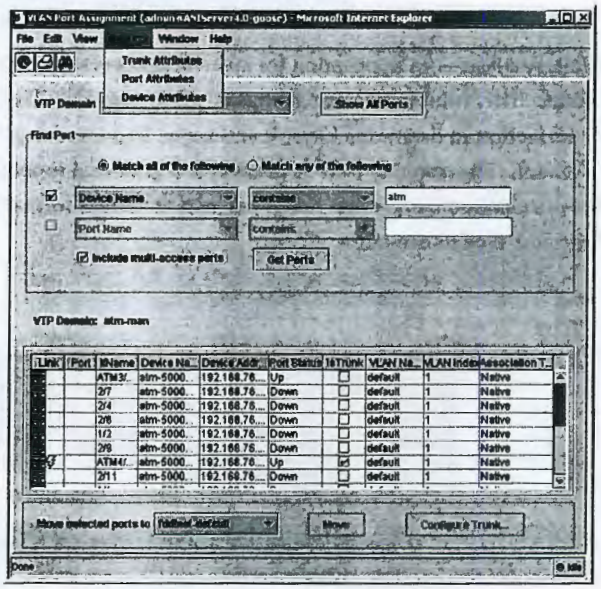
RQS Nº 03/2005 - CN
CPMI - CORREIOS
0324
Fls:
3701
Doc:

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

VLAN/LANE Configuration and Port Assignment

Campus Manager provides an easy and graphical means for creating, modifying, or deleting VLANs, LANE elements, or assigning switch ports to VLANs. As VLANs are created or modified, port and user changes are instantly updated and transmitted to the switches, eliminating the need to update and configure each participating switch individually. As VLANs are selected, the table view shows the participating ports, port status, and switch information and the topology map can be launched to graphically highlight participating devices and links of the VLAN connections. Additional map tools allow managers to show spanning-tree states, VTP trunks, switch port links, and existing LANE service elements.

Figure 8
VLAN Port Assignment



Campus Manager 3.3 is a must for switched network management, and is an integral piece of the LAN Management Solution, by providing a broad, comprehensive set of tools for managing and administering the entire LAN environment.

Campus Manager 3.3 Features

Campus Manager provides a variety of functions within Topology Services, User Tracking, Path Analysis and VLAN/LANE port assignment that network managers can use to better understand, monitor, configure, diagnose, and be proactive to network infrastructure changes.

Topology Services

Topology Services provides access to a wide variety of physical and logical topology maps, summary lists of devices, ports, and their network relationships. Topology Services also acts as the launching point for topology-related configuration and diagnostic tools.

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

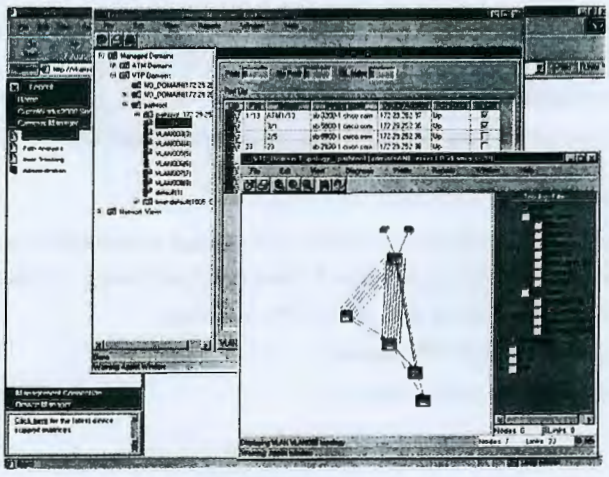
2558
Fls.

In Campus Manager 3.3, network topology maps can be displayed in a variety of ways from both a flat Layer 2 to abstracted views that better represent and scale to large campus networks. These abstractions are categorized into three different groups: managed domains, network views and topology groups. Managed domains are topological views of logical groups of devices organized around ATM switch fabrics and VTP domains. Network views are physical displays of the network and are organized to provide full and abstracted views, such as LAN edge views, Layer 2 views, unconnected device views, and VTP views. Topology Groups are custom views that are a subset of the entire network based on the group rule defined while creating the view. They are can be two types of groups—system defined groups that are custom views created by admin user and user defined views which are created by CiscoWorks users. Membership to these groups are made via rules that can be evaluated either automatically or upon user request and these groups help in generating custom views that are a subset of the Layer 2 views.

Key features in the Campus Manager topology services include:

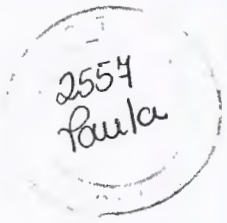
- Autodiscovery and display of Cisco switches, routers, and probes using the Cisco Discovery Protocol (CDP) and SNMP
- Display of physical and logical Layer 2 connections within the discovered LAN environment
- Highlighting tools to identify specific classes of devices or links such as switches, route switch modules (RSMs), Fast Ethernet, EtherChannel®, ATM links, Cisco Customer Response Applications, and other relevant Cisco device elements
- Expanded scalability to support more than 2000 Cisco devices
- Display of multilayer switches and components (switching entities and route-processing entities) with the ability to highlight logical relationships between devices, such as flow masks and shortcuts
- Device status indicators on the topology maps based on CDP, ILMI, ELMI, and SNMP availability
- Automated discrepancy reporting during discovery highlights connection problems, link mismatches, and logical misconfigurations
- Graphical interface for creating VLAN and LANE services for Ethernet, Token Ring, and transparent VLANs
- Graphical interface for locating—through search parameters—and assigning switch ports individually or in bulk to a VLAN
- ATM soft PVC configuration and diagnostics

Figure 9
Topology Views and Tools



All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0325
Fls:
3701
Doc:



VLAN/LANE Configuration and Port Assignment

Campus Manager provides an easy and graphical means for creating, modifying, or deleting VLANs, LANE elements, or assigning switch ports to VLANs. As VLANs are created or modified, port and user changes are instantly updated and transmitted to the switches, eliminating the need to update and configure each participating switch individually. As VLANs are selected, the table view shows the participating ports, port status, and switch information and the topology map can be launched to graphically highlight participating devices and links of the VLAN connections. Additional map tools allow managers to show spanning-tree states, VTP trunks, switch port links, and existing LANE service elements.

VLAN management services provide:

- Tabular summary views of VLANs shows participating ports, devices, links, and port status information
- Graphical setup of VLANs (including transparent VLANs) and VLAN membership to simplify administration
- Integration of LANE configuration services in VLAN configuration tools for more efficient operational and engineering practices
- A separate interface for administrators to quickly search, using a variety of criteria, and assign selected switch ports, individually or in bulk, to VLANs
- Logical display of VLAN configurations makes it easy to visualize switch connections
- Automated discrepancy reports highlight connection problems and link mismatches
- Automated VLAN membership registration reduces administration and configuration requirements

ATM Management

Campus Manager offers a graphical tool for managing complex ATM networks, simplifying configuration and performance monitoring. ATM networks are displayed on the topology map and the logical VLAN and ATM domain views provide graphical representations of ATM switches and LANE elements. "Drill down" capability allows access to configuration and performance monitoring tools. ATM management functions include:

- Autodiscovery of ATM switches, including switched virtual circuit (SVC) and PVC connections
- Connectivity checking of SVC and PVC connections
- End-to-end virtual circuit path tracing and analysis, which assists in connectivity diagnostics
- LANE troubleshooting and performance analysis
- Quality of service (QoS) templates for simplifying the configuration of typical traffic such as video or constant-bit-rate (CBR)
- Simple configuration of soft PVCs
- ATM remote monitoring (RMON) data collection and analysis

User Tracking

User Tracking automatically locates servers and end-user workstations, and Cisco voice over IP (VoIP) telephone handsets and their connections to Layer 2 Cisco switches. During this discovery process it also tabulates specific connection information about that end station, including:

- VLAN name, type, and VTP domain
- Switch port number, name, and state

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

2556
Paula

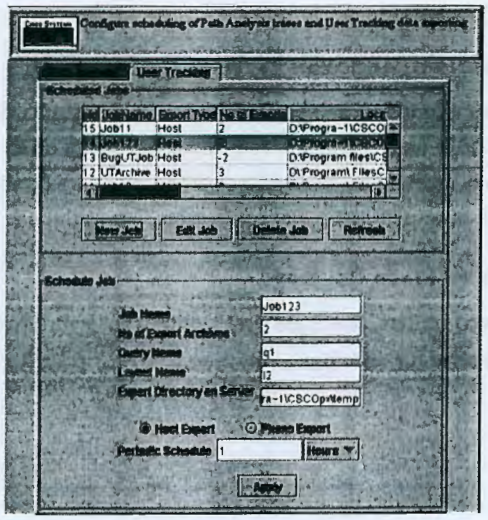
- MAC and IP address of the end station and its subnet
- Tabular and sortable listing of all switch port attached end-user workstations, servers and IP handsets
- Last-seen time stamp reflecting last acquisition in which the end station was detected
- User login name passed automatically from the Windows NT Primary Domain Controller or Novell Directory Structure, or from the UNIX host

Campus Manager simplifies the dynamic nature of many business environments by providing a large number of sortable parameters that can be used to locate end-user stations. User Tracking discovers end stations connected to switch ports automatically and provides a means to identify end users, their assigned VLANs, and host station connections. User Tracking also supports voice/data convergence with interfaces to Cisco CallManager for correlating the IP and MAC addresses of discovered VoIP handsets with their assigned phone number and users.

User Tracking provides the following features:

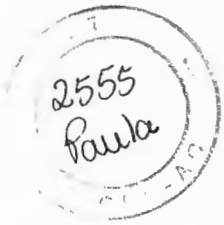
- Enhanced scalability to support 60,000 end stations
- Predefined reports that identify duplicate MAC and IP addresses, ports with multiple MAC addresses and duplicate sysnames.
- IP and MAC addresses of discovered VoIP handsets with their assigned phone number and users
- Tabular and sortable listing of all switch port-attached end-user workstations and IP handsets
- Customized tables for user-defined, detailed reporting
- GUI for user tracking information table configuration to support dynamic/mobile users
- Scheduling managers for automating address change updates
- Easy-to-use search utility box locating users by MAC addresses, IP addresses, DNS host names, switch port labels, and optional voice handsets
- Provides ability to schedule User Tracking. Also exports User Tracking reports.
- Ability to define acquisition based on a subnet range

Figure 10
Scheduled export of User Tracking Reports



Cisco Systems, Inc.
All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

...JS Nº 03/2005 - CN
CPMI - CORREIOS
0326
Fls:
3701



Path Analysis

Path Analysis is a powerful diagnostic tool for determining the Layer 2 and Layer 3 path between two selected endpoints using Campus Manager-discovered end-station data, VLAN/LANE configuration information, real-time Layer 3 path trace information, and spanning-tree calculations. Displays of path information are available in both topological map and tabular displays. Key Path Analysis features include:

- View the Layer 2 and Layer 3 path information in a map format with traces showing end stations, Layer 2 and 3 devices, route directions, and cut-through paths
- View specific details of the Layer 2 and Layer 3 path, including IP addresses and interfaces traveled, VLAN and VTP domain names, and port speeds and duplex settings
- Perform traces immediately or schedule them
- Perform traces using IP address, DNS name, or by telephone number for voice calls as start/stop points
- Provide Layer 2 and Layer 3 trace information between Cisco voice elements using interfaces to call detail records for specific voice calls
- Provides ability to schedule path traces. Also exports path traces data.

Built on the CiscoWorks Management Server

The CiscoWorks management server provides common resources, such as Web services, discovery, shared databases and database services, and the management desktop. Cisco Management Connection, a service on the CiscoWorks2000 server, delivers a set of tools for integrating applications into the management desktop using Internet-based standards and technologies. These tools allow users to link Web-based management applications to the CiscoWorks family of products and application developers to easily link Web-based applications through a certified registration mechanism. Cisco Management Connection has been used by Cisco and more than 30 network management vendors, including Hewlett-Packard, Computer Associates, Sun Microsystems, and Tivoli Systems to create certified Cisco Management Connections for their applications. This rapid adoption has created an environment in which users can easily build management intranets that link together their favorite Web-based management applications.

Specifications

Server, Client, and Web Browser System Requirements

The server, client and web browser system requirements can be found in the Product Overview documents for the Routed WAN and LAN Management solutions and on Cisco's main on-line documentation site, under each CiscoWorks solution. Please refer to these and other Product Installation documentation for more detailed information on setting up and configuring these solutions.

Supported Cisco Devices

Most Cisco routers, Catalyst® and LightStream switches, as well as Cisco AVVID devices. Contact your Cisco representative for a complete list.

Cisco Systems, Inc.
All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Supported Cisco IOS Versions

- Cisco IOS® version 10.3 and above
- Catalyst Supervisor code 2.1 and above

Availability

Campus Manager 3.3 is an integral part of multiple CiscoWorks solutions and is not sold as an individual product. For additional information on Campus Manager, see:
http://cisco.com/warp/public/cc/pd/wr2k/

2554
Paula

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

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Catalyst, Cisco, Cisco IOS, Cisco Systems, the Cisco Systems logo, and EtherChannel are trademarks or registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0303R)

803046/ETMO/0340

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0327
Fls: 3701
Doc:

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0328
Fls:
370
Doc:

Apendice AI

2553
Rauka

Cisco Systems

Data Sheet

CiscoWorks **Campus Manager**

Campus Manager is a key component in the CiscoWorks family of management solutions designed to make Cisco networks the most manageable and available in the industry. Today's networks are critical business assets, and require sophisticated tools for administering, monitoring and configuring Layer 2 services. Designed for enterprise network operations staff, Campus Manager provides powerful tools with built-in network intelligence to reduce the complexity and automate manual tasks associated with maintaining complex physical and logical network infrastructures.

Campus Manager Overview

Campus networks are at the heart of business and mission-critical systems. The requirement to understand, monitor, and react to changing networking conditions drives the need for sophisticated, yet easy-to-use management tools. Campus Manager is part of the LAN Management Solution, part of the broad range of CiscoWorks network management solutions.

New in Version 3.3:

In addition to the rich set of management features already included, the new version of Campus Manager has been enhanced to provide even greater manageability for Cisco networks. New benefits include:

- Improved application performance
- Doubled capacity for tracking end users

Key Campus Manager features include:

- Intelligent discovery and display of Layer 2 networks on browser-accessible topology maps, independent of VTP server
- Configuration of virtual LAN (VLAN)/ LAN Emulation (LANE) and asynchronous transfer mode (ATM) services and assignment of switch ports to those services
- Link and device status display based upon Simple Network Management Protocol (SNMP) polling
- Identification of Layer 2 configuration discrepancies
- Diagnostic tools for connectivity related problems between end stations, and Layer 2 and Layer 3 devices
- Automatic location and correlation of information on users by media access control (MAC), IP address, NT or NetWare Directory Services (NDS) login or UNIX host name, with their physical connections to the switched network
- Visibility and launch point of Cisco CallManager from topology services as well as tracking of phone handset to IP, Mac address, and switch port
- Layer 2 and Layer 3 path trace between source and destination handsets
- Export of topology maps to Visio
- Java plugins to improve graphical user interface (GUI) performance

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0320
Fls:
3701
Doc:

Cisco Systems, Inc.
All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

2552
Paula

- Ability to form Custom Groups in Topology View based on criteria like SysLocation, SysName and IP address/ Subnet mask.
- Secure communication between the client browser and Campus applications using Secure Socket Layer (SSL) protocol.

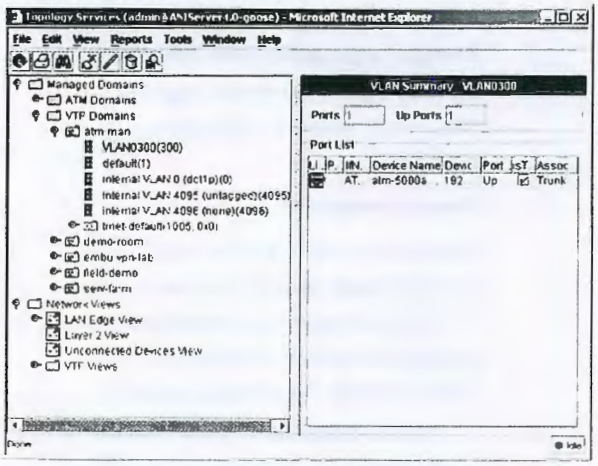
Campus Manager enables administrators to more easily change, monitor, and control network relationships, making them more effective in delivering business-critical and advanced networking services to their users and customers.

Campus Manager is a suite of applications launched from a common "management desktop" used by all Web-based CiscoWorks applications. Campus Manager contains three applications that can be launched from the client's browser:

- Topology Services—This is the principal interface to a variety of large scale topology maps, tabular summaries, reports, and configuration services of the Layer 2 network. A directory-like tree interface lists physical Layer 2 and logical, Virtual Trunking Protocol (VTP), and ATM domain views along with table summaries of the devices and interface associated with these views. This tree structure acts as the launching point for topology maps, discrepancy reporting functions, and configuration services. The integrated VLAN and LANE configuration capabilities, ATM soft permanent virtual circuit (PVC) configuration and diagnostic tools, along with physical and logical configuration discrepancy checking reports and highlighting tools are found within the Topology Services menus. It also supports discovery and display of Cisco Customer Response Applications, and reports on services of these devices.

  Ability to form custom groups based on dynamic and static rules for the group membership. System defined groups and user defined grouping can be created by network administrators and users respectively and allows grouping by developing rules based on criteria such as IP address, subnets, SysLocation, SysName, SysContact, Image Version and hostname. A rules editor allows for creating, editing Topology groups and defines rules for membership.

Figure 1
Topology Services Tabular View



Cisco Systems, Inc.
All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

2551
Paula

Figure 2
VTP Domain Topology Map

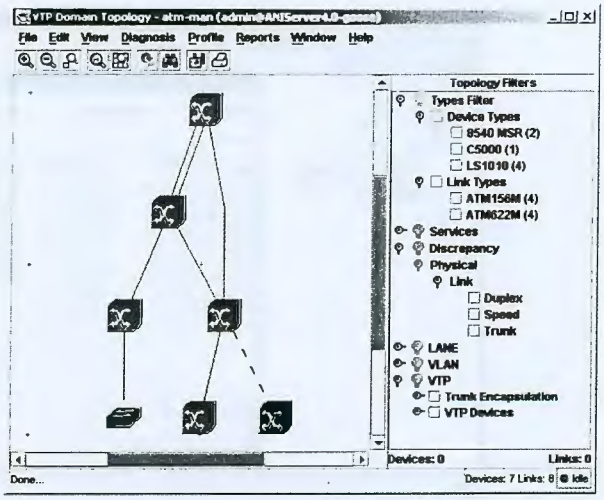
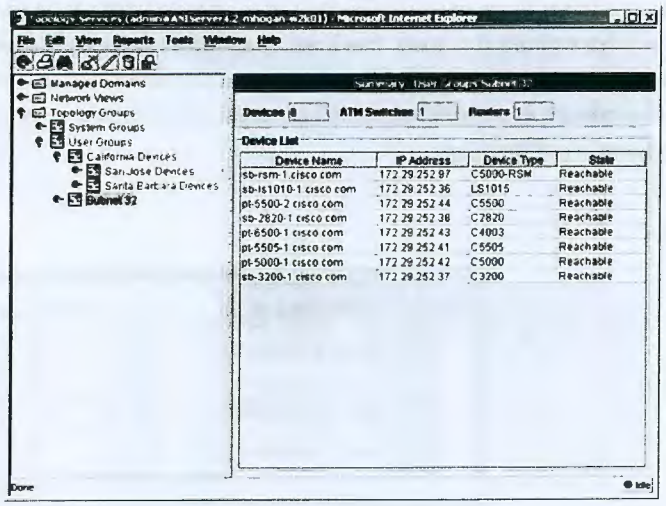


Figure 3
Forming Topology Groups

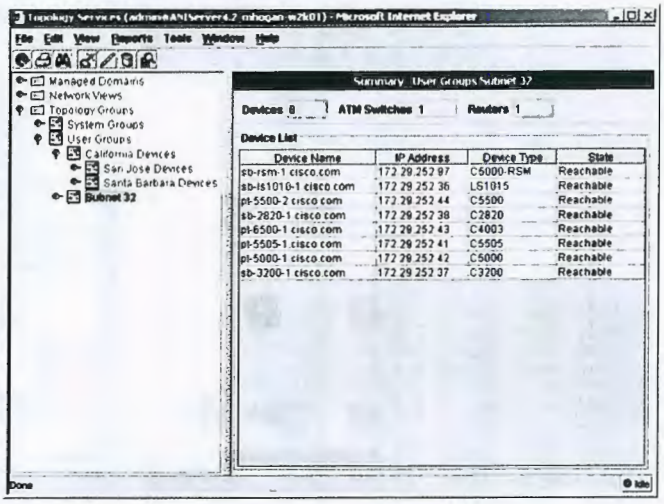


All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0330
Fls: 3701
Doc:

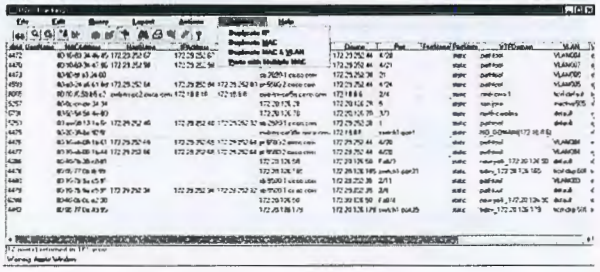
2550
Paula

Figure 4
Topology Group in Topology Maps



- User Tracking—Designed to assist in locating end-station connections at the access switch, this application is a useful tool in troubleshooting or connectivity analysis. Through automated acquisition, a table of end-user stations and Layer 2 connection information is constructed. This table can be sorted and queried allowing administrators to easily find users. Users can be identified by name, IP handset, MAC and IP address, as well as the switch port and switch that they are connected, along with VLAN and VTP assignment of the port. Predefined reports, such as duplicate MAC per switch port, or duplicate IP addresses, enable managers to locate mobile users or violations in port policies.

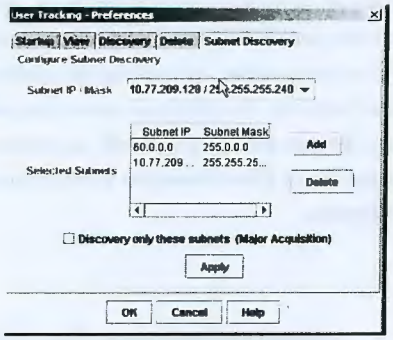
Figure 5
User Tracking



All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

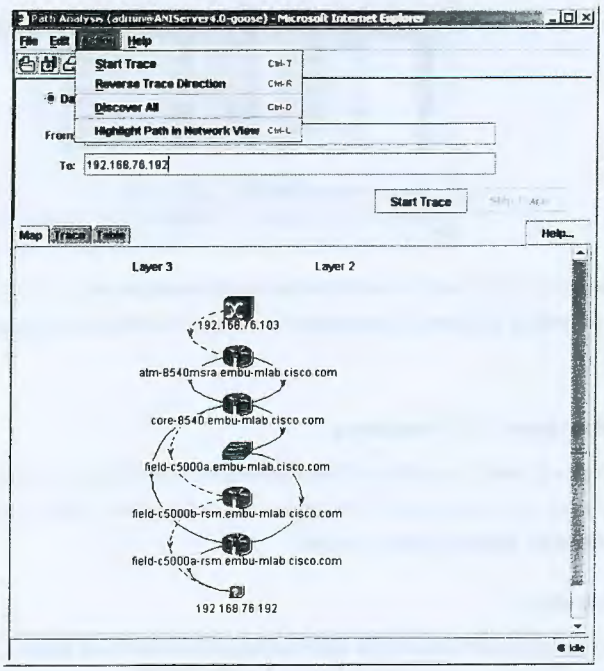
2549
Paula

Figure 6
Subnet based acquisition



- Path Analysis—An application for switched network management, this is an extremely powerful tool for connectivity troubleshooting. Path Analysis utilizes User Tracking, topology services, and real-time spanning tree information to determine Layer 2 and Layer 3 connectivity between two end-points, or IP Handsets, in the network. The resulting trace is presented in graphical topology views that illustrate the Layer 2 and Layer 3 devices, path direction and link types, and in tabular formats that provide specific interface, IP address, VLAN, and link type information.

Figure 7
Path Analysis



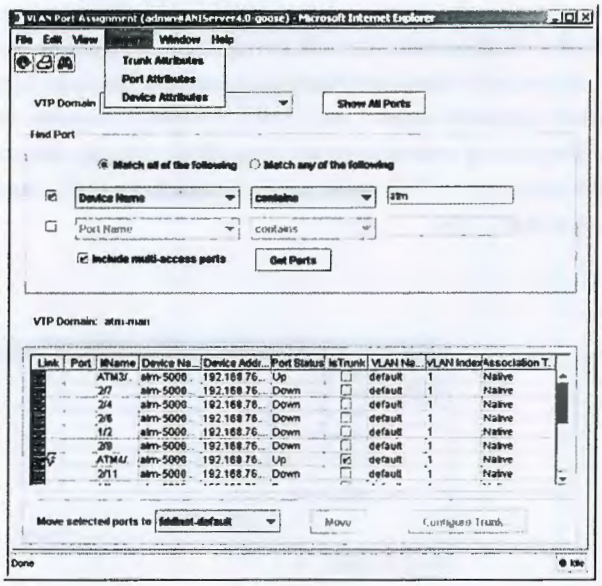
All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

ROS Nº 03/2005 - CN
CPMI - CORREIOS
0331
Fls:
Doc:
3701

VLAN/LANE Configuration and Port Assignment

Campus Manager provides an easy and graphical means for creating, modifying, or deleting VLANs, LANE elements, or assigning switch ports to VLANs. As VLANs are created or modified, port and user changes are instantly updated and transmitted to the switches, eliminating the need to update and configure each participating switch individually. As VLANs are selected, the table view shows the participating ports, port status, and switch information and the topology map can be launched to graphically highlight participating devices and links of the VLAN connections. Additional map tools allow managers to show spanning-tree states, VTP trunks, switch port links, and existing LANE service elements.

Figure 8
VLAN Port Assignment



Campus Manager 3.3 is a must for switched network management, and is an integral piece of the LAN Management Solution, by providing a broad, comprehensive set of tools for managing and administering the entire LAN environment.

Campus Manager 3.3 Features

Campus Manager provides a variety of functions within Topology Services, User Tracking, Path Analysis and VLAN/LANE port assignment that network managers can use to better understand, monitor, configure, diagnose, and be proactive to network infrastructure changes.

Topology Services

Topology Services provides access to a wide variety of physical and logical topology maps, summary lists of devices, ports, and their network relationships. Topology Services also acts as the launching point for topology-related configuration and diagnostic tools.

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

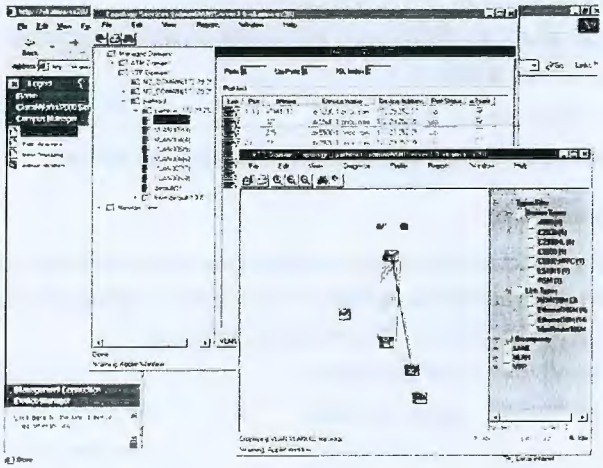
2547
Paula

In Campus Manager 3.3, network topology maps can be displayed in a variety of ways from both a flat Layer 2 to abstracted views that better represent and scale to large campus networks. These abstractions are categorized into three different groups: managed domains, network views and topology groups. Managed domains are topological views of logical groups of devices organized around ATM switch fabrics and VTP domains. Network views are physical displays of the network and are organized to provide full and abstracted views, such as LAN edge views, Layer 2 views, unconnected device views, and VTP views. Topology Groups are custom views that are a subset of the entire network based on the group rule defined while creating the view. They are can be two types of groups—system defined groups that are custom views created by admin user and user defined views which are created by CiscoWorks users. Membership to these groups are made via rules that can be evaluated either automatically or upon user request and these groups help in generating custom views that are a subset of the Layer 2 views.

Key features in the Campus Manager topology services include:

- Autodiscovery and display of Cisco switches, routers, and probes using the Cisco Discovery Protocol (CDP) and SNMP
- Display of physical and logical Layer 2 connections within the discovered LAN environment
- Highlighting tools to identify specific classes of devices or links such as switches, route switch modules (RSMs), Fast Ethernet, EtherChannel®, ATM links, Cisco Customer Response Applications, and other relevant Cisco device elements
- Expanded scalability to support more than 2000 Cisco devices
- Display of multilayer switches and components (switching entities and route-processing entities) with the ability to highlight logical relationships between devices, such as flow masks and shortcuts
- Device status indicators on the topology maps based on CDP, ILMI, ELMI, and SNMP availability
- Automated discrepancy reporting during discovery highlights connection problems, link mismatches, and logical misconfigurations
- Graphical interface for creating VLAN and LANE services for Ethernet, Token Ring, and transparent VLANs
- Graphical interface for locating—through search parameters—and assigning switch ports individually or in bulk to a VLAN
- ATM soft PVC configuration and diagnostics

Figure 9
Topology Views and Tools



All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0332
Fls:
3701
Doc:

VLAN/LANE Configuration and Port Assignment

Campus Manager provides an easy and graphical means for creating, modifying, or deleting VLANs, LANE elements, or assigning switch ports to VLANs. As VLANs are created or modified, port and user changes are instantly updated and transmitted to the switches, eliminating the need to update and configure each participating switch individually. As VLANs are selected, the table view shows the participating ports, port status, and switch information and the topology map can be launched to graphically highlight participating devices and links of the VLAN connections. Additional map tools allow managers to show spanning-tree states, VTP trunks, switch port links, and existing LANE service elements.

VLAN management services provide:

- Tabular summary views of VLANs shows participating ports, devices, links, and port status information
- Graphical setup of VLANs (including transparent VLANs) and VLAN membership to simplify administration
- Integration of LANE configuration services in VLAN configuration tools for more efficient operational and engineering practices
- A separate interface for administrators to quickly search, using a variety of criteria, and assign selected switch ports, individually or in bulk, to VLANs
- Logical display of VLAN configurations makes it easy to visualize switch connections
- Automated discrepancy reports highlight connection problems and link mismatches
- Automated VLAN membership registration reduces administration and configuration requirements

ATM Management

Campus Manager offers a graphical tool for managing complex ATM networks, simplifying configuration and performance monitoring. ATM networks are displayed on the topology map and the logical VLAN and ATM domain views provide graphical representations of ATM switches and LANE elements. "Drill down" capability allows access to configuration and performance monitoring tools. ATM management functions include:

- Autodiscovery of ATM switches, including switched virtual circuit (SVC) and PVC connections
- Connectivity checking of SVC and PVC connections
- End-to-end virtual circuit path tracing and analysis, which assists in connectivity diagnostics
- LANE troubleshooting and performance analysis
- Quality of service (QoS) templates for simplifying the configuration of typical traffic such as video or constant-bit-rate (CBR)
- Simple configuration of soft PVCs
- ATM remote monitoring (RMON) data collection and analysis

User Tracking

User Tracking automatically locates servers and end-user workstations, and Cisco voice over IP (VoIP) telephone handsets and their connections to Layer 2 Cisco switches. During this discovery process it also tabulates specific connection information about that end station, including:

- VLAN name, type, and VTP domain
- Switch port number, name, and state

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

2545 Paula

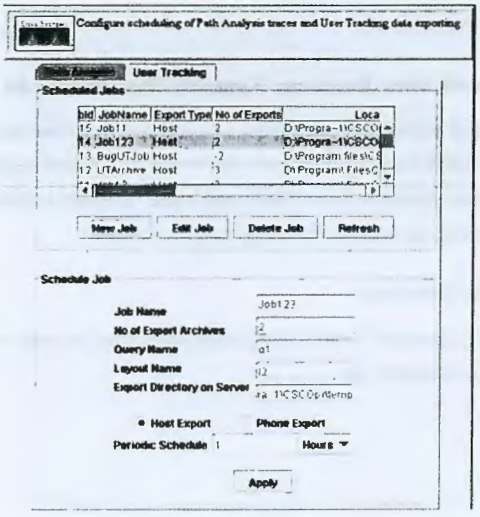
- MAC and IP address of the end station and its subnet
- Tabular and sortable listing of all switch port attached end-user workstations, servers and IP handsets
- Last-seen time stamp reflecting last acquisition in which the end station was detected
- User login name passed automatically from the Windows NT Primary Domain Controller or Novell Directory Structure, or from the UNIX host

Campus Manager simplifies the dynamic nature of many business environments by providing a large number of sortable parameters that can be used to locate end-user stations. User Tracking discovers end stations connected to switch ports automatically and provides a means to identify end users, their assigned VLANs, and host station connections. User Tracking also supports voice/data convergence with interfaces to Cisco CallManager for correlating the IP and MAC addresses of discovered VoIP handsets with their assigned phone number and users.

User Tracking provides the following features:

- Enhanced scalability to support 60,000 end stations
- Predefined reports that identify duplicate MAC and IP addresses, ports with multiple MAC addresses and duplicate sysnames.
- IP and MAC addresses of discovered VoIP handsets with their assigned phone number and users
- Tabular and sortable listing of all switch port-attached end-user workstations and IP handsets
- Customized tables for user-defined, detailed reporting
- GUI for user tracking information table configuration to support dynamic/mobile users
- Scheduling managers for automating address change updates
- Easy-to-use search utility box locating users by MAC addresses, IP addresses, DNS host names, switch port labels, and optional voice handsets
- Provides ability to schedule User Tracking. Also exports User Tracking reports.
- Ability to define acquisition based on a subnet range

Figure 10
Scheduled export of User Tracking Reports



All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

ROS Nº 03/2005 - CN
CPMI - CORREIOS
0333
Fls: 3701
Doc:

Path Analysis

Path Analysis is a powerful diagnostic tool for determining the Layer 2 and Layer 3 path between two selected endpoints using Campus Manager-discovered end-station data, VLAN/LANE configuration information, real-time Layer 3 path trace information, and spanning-tree calculations. Displays of path information are available in both topological map and tabular displays. Key Path Analysis features include:

- View the Layer 2 and Layer 3 path information in a map format with traces showing end stations, Layer 2 and 3 devices, route directions, and cut-through paths
- View specific details of the Layer 2 and Layer 3 path, including IP addresses and interfaces traveled, VLAN and VTP domain names, and port speeds and duplex settings
- Perform traces immediately or schedule them
- Perform traces using IP address, DNS name, or by telephone number for voice calls as start/stop points
- Provide Layer 2 and Layer 3 trace information between Cisco voice elements using interfaces to call detail records for specific voice calls
- Provides ability to schedule path traces. Also exports path traces data.

Built on the CiscoWorks Management Server

The CiscoWorks management server provides common resources, such as Web services, discovery, shared databases and database services, and the management desktop. Cisco Management Connection, a service on the CiscoWorks2000 server, delivers a set of tools for integrating applications into the management desktop using Internet-based standards and technologies. These tools allow users to link Web-based management applications to the CiscoWorks family of products and application developers to easily link Web-based applications through a certified registration mechanism. Cisco Management Connection has been used by Cisco and more than 30 network management vendors, including Hewlett-Packard, Computer Associates, Sun Microsystems, and Tivoli Systems to create certified Cisco Management Connections for their applications. This rapid adoption has created an environment in which users can easily build management intranets that link together their favorite Web-based management applications.

Specifications

Server, Client, and Web Browser System Requirements

The server, client and web browser system requirements can be found in the Product Overview documents for the Routed WAN and LAN Management solutions and on Cisco's main on-line documentation site, under each CiscoWorks solution. Please refer to these and other Product Installation documentation for more detailed information on setting up and configuring these solutions.

Supported Cisco Devices

Most Cisco routers, Catalyst® and LightStream switches, as well as Cisco AVVID devices. Contact your Cisco representative for a complete list.

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Supported Cisco IOS Versions

- Cisco IOS® version 10.3 and above
- Catalyst Supervisor code 2.1 and above

Availability

Campus Manager 3.3 is an integral part of multiple CiscoWorks solutions and is not sold as an individual product. For additional information on Campus Manager, see:
http://cisco.com/warp/public/cc/pd/wr2k/

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

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Catalyst, Cisco, Cisco IOS, Cisco Systems, the Cisco Systems logo, and EtherChannel are trademarks or registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0303R)

CCMP/ETMG 03/03

ROS Nº 03/2005 4CN
CPMI - CORREIOS
0334
Fls:
3701
Doc:

Apêndice AJ

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 0335
Doc: 3701

2542
Paula

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.

Reprinted with permission from *Packet*™ magazine (Volume 13, No. 1), copyright © 2001 by Cisco Systems,Inc. All rights reserved.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0336
Fls:
3701
Doc:

2511 Paulo

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 535 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.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
CISCO SYSTEMS 0337
Fls:
3701
Doc:

2540
Paula

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

Reprinted with permission from *Packet*™ magazine (Volume 13, No. 1), copyright © 2001 by Cisco Systems,Inc. All rights reserved.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0338
Fls:
Doc: 3701

Apêndice AL

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0339
Fls: 3701
Doc:

2539 Paula

Cisco Systems

Data Sheet

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.

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

Figure 1
Cisco PIX 525 Security Appliance

ROS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 0340
Doc: 3701

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

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.

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

2537
Paula

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

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS nº 03/2005 - CN
CPMI - CORREIOS
0341
Fls:
Doc 3701

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

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

2535
Paula

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+)

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 0342
Doc: 3701

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

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

2533
Paula

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)

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0343
Fls:
3701
Doc:

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+

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

2531
Paulo

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

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS Nº 03/2005 - CN
CRMI - CORREIOS
0344
Fls:
Doc: 3701

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

2530 Paula

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

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

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. CCIP, CCSP, the Cisco Arrow logo, the Cisco *Powered* Network mark, Cisco Unity, Follow Me Browsing, FormShare, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherSwitch, Fast Step, GigaStack, Internet Quotient, IOS, IP/TV, IQ Expertise, the IQ logo, IQ Net Readiness Scorecard, LightStream, MGX, MICA, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, RateMUX, Registrar, ScriptShare, SlideCast, SMARTnet, StrataView Plus, Stratm, SwitchProbe, TeleRouter, The Fastest Way to Increase Your Internet Quotient, TransPath, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0304R)

RD/LW3946 04/03

Apenso XVI

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0345
Fls:
Doc: 3701

2529
Paula

Data Sheet

Firewall Services Module for Cisco Catalyst® 6500 Series and Cisco 7600 Series

The Firewall Services Module (FWSM)—a high-speed, integrated firewall module for Cisco Catalyst® 6500 switches and Cisco 7600 Series routers—provides the fastest firewall data rates in the industry: 5 Gb throughput, 100,000 CPS, and 1M concurrent connections. Up to four FWSMs can be installed in a single chassis providing scalability to 20 GB per chassis. As part of the world-leading Cisco PIX® Firewall family, the FWSM provides large enterprises and service providers with unmatched security, reliability, and performance.

The FWSM leverages Cisco PIX technology and runs the Cisco PIX Operating System (OS), a real-time, hardened, embedded system that eliminates security holes and performance-degrading overhead. At the heart of the system, a protection scheme based on the Adaptive Security Algorithm (ASA) offers stateful connection-oriented firewalling. Using ASA, the FWSM creates a connection table entry for a session flow based on the source and destination addresses, randomized TCP sequence numbers, port numbers, and additional TCP flags. The FWSM controls all inbound and outbound traffic by applying the security policy to these connection table entries.

Figure 1

Major FWSM Benefits

The traditional role of firewalls has changed. Firewalls now do more than protect a corporate network from unauthorized external access. They can also prevent unauthorized users from accessing a particular subnet, workgroup or LAN within a corporate network. FBI statistics indicate that 70 percent of all security problems originate from inside an organization. According to one in five respondents to the FBI's survey, intruders broke into, or tried to break into their corporate networks during the preceding 12 months. And most experts agree that the majority of network break-ins go undetected.

Integrated Module

Installed inside a Cisco Catalyst 6500 Series Switch or Cisco 7600 Internet Router, the FWSM allows any port on the device to operate as a firewall port and integrates stateful firewall security inside the network infrastructure. This becomes especially important where rack space is at a premium. The Cisco Catalyst 6500 truly emerges as the IP services switch of choice for customers requiring intelligent services

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0346
Fls:
Doc: 3701

such as firewall services, intrusion detection, and virtual private networking (VPN), along with multilayer LAN, WAN, and MAN switching capabilities.

Future Proof

The FWSM can handle up to 5 Gb of traffic, providing unsurpassed performance to meet future requirements without requiring a system overhaul. Up to three additional FWSMs can be added to the Catalyst 6500 to meet growing demands.

Reliability

The FWSM is based on Cisco PIX technology and uses the same time-tested Cisco PIX Operating System, a secure, real-time operating system. The FWSM offers a unique combination of performance and security on the same platform, using proven Cisco PIX technology for inspecting packets.

Lower Cost of Ownership

The FWSM offers the best price/performance of any firewall. Cost of maintenance is included in the SmartNet™ contract of the Cisco Catalyst chassis. Because the FWSM is based on the Cisco PIX Firewall, the cost of training and management is lower, and because it is integrated in the chassis, there are fewer boxes to manage.

Ease of Use

The Cisco PIX Device Manager's intuitive graphical user interface (GUI) can be used to manage and configure the FWSM. The FWSM is supported by the Cisco management framework and by Cisco AVVID (Architecture for Voice, Video and Integrated Data) partners for configuration and monitoring.

FWSM Features

Key Features	Benefits
Performance	• 5 Gbps • 1 million concurrent connections • More than 100,000 connection setup and teardowns/sec
Multiple Interfaces	• Supports up to 100 firewall VLANs—any of the Cisco Catalyst 4000 VLANs can be a firewall VLAN • Understands 802.1q and Inter-Switch Link (ISL) protocols
Cut-through Proxies	Enforces security policies on a per VLAN basis

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0347
Fls:
Doc:

Key Features	Benefits
Configuration Support	• Console to command-line interface (CLI) • Telnet to the inside interface of the Cisco PIX Firewall • Telnet over IP Security (IPSec) to the outside interface of the Cisco PIX Firewall • Secure Shell Protocol (SSH) to CLI • Secure Sockets Layer (SSL) to Cisco PIX Device Manager
AAA Support	Integrates with popular authentication, authorization, and accounting services via TACACS+ and RADIUS support
NAT/PAT Support	Provides dynamic/static Network Address Translation (NAT) and Port Address Translation (PAT)
Cisco PIX Device Manager (PDM)	• Simple, intuitive, Web-based GUI supports remote firewall management • Wide range of real-time and historical reports providing usage trend, performance baseline, and security event information
Secure Network Management	Secure, Triple Data Encryption Standard (3DES)-encrypted network management access
Access Lists	• Up to 128,000 access lists
URL Filtering	Uses Websense software to check outgoing URL requests with the policies defined on the server
Command Authorization	Allows privilege levels to be assigned to all CLI, and creation of user accounts or login contexts tied to these privilege levels
Object Grouping	Ability to group network objects (e.g., hosts) and services (e.g., ftp and http)
Protection from DoS	• DNS Guard • Flood Defender • Flood Guard • TCP Intercept • Unicast Reverse Path Forwarding • Mail Guard • FragGuard and Virtual Reassembly
Routing	• Static routes • Dynamic; i.e., Routing Interface Protocol (RIP) and Open Shortest Path First (OSPF)
High Availability	Stateful failover—intra and interchassis
Logging	Comprehensive syslogging, FTP, URL, and ACL logging
Additional Protocols	• H.323 V2 • NetBios over IP • RAS Version 2 • RTSP • SIP • XDMCP • Skinny

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement

RDSAN° 03/2005 - CN
CPMI - CORREIOS
0348
Fls:
Doc: 3701

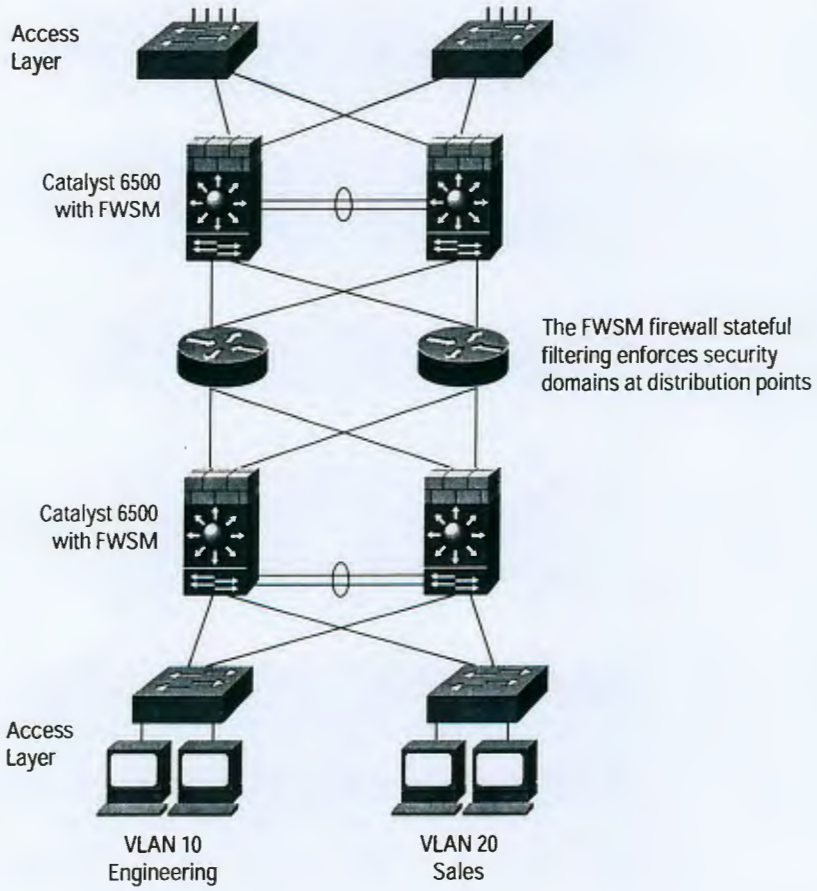
2526
Paula

FWSM Deployment

The FWSM can be deployed in topologies serving enterprise campuses and data centers.

Today's Enterprises need more than just perimeter security—they need to connect business partners and provide campus security domains that serve multiple groups within the organizations. The FWSM provides a flexible, cost-effective and performance-based solution by allowing users and administrators to establish security domains with different policies within the organization. Figure 2 shows a campus deployment using stateful filtering to establish separate VLAN-based security domains:

Figure 2
Campus Deployment



Using the FWSM, users can set appropriate policies for different VLANs.

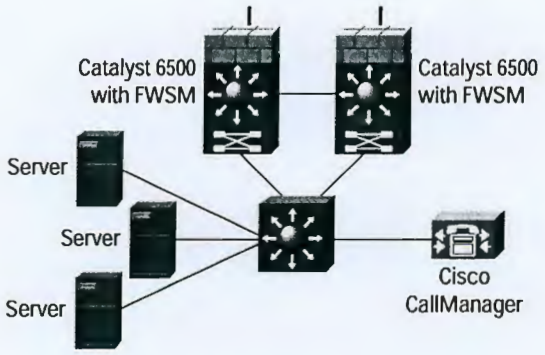
Data Centers also require stateful firewall security solutions to protect data while delivering gigabit performance at the lowest possible cost. Figure 2 shows a data center with redundant FWSMs protecting server data.

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0349
Fls:
3701
Doc:

2525 Paula

Figure 3
eCommerce Data Center Deployment



The FWSM maximizes capital investment by providing the best price/performance in a firewall and allows customers to replace expensive multiple firewalls that require additional firewall load balancer devices.

Ordering Information

Product Number	Description
WS-SVC-FWM-1-K9	Firewall Service Module for Cisco Catalyst 6500
WS-SVC-FWM-1-K9=	Firewall Service Module for Cisco Catalyst 6500 (spare)
SC-SVC-FWM-1.1-K9	Firewall Module Software for Catalyst 6500
SC-SVC-FWM-1.1-K9=	Firewall Module Software for Catalyst 6500 (spare)

Licensing

No licensing is required for the FWSM.

System Requirements

- Supervisor 2/Multilayer Switch Feature Card 2 (MSFC2)
- Native Cisco IOS® software release 12.1(13)E or higher
- Hybrid CatOS minimum software release 7.5(1)
- Occupies one slot in a Cisco Catalyst 6500 Series Switch or Cisco 7600 Series Internet Router
- Up to four firewall modules in the same chassis

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0350
Fls:
Doc: 3701

Regulatory Compliance

Safety

- UL 1950
- CSA C22.2 No. 950-95
- EN60950
- EN60825-1
- TS001
- CE Marking
- IEC 60950
- AS/NZS3260

EMI

- FCC Part 15 Class A
- ICES-003 Class A
- VCCI Class B
- EN55022 Class B
- .R22 Class B
- CE Marking
- AS/NZS3548 Class B

NEBS

- SR-3580 - NEBS: Criteria Levels (Level 3 compliant)
- GR-63-CORE - NEBS: Physical Protection
- GR-1089-CORE - NEBS: EMC and Safety

ETSI

- ETS-300386-2 Switching Equipment

Telecommunications

- ITU-T G.610
- ITU-T G.703
- ITU-T G.707
- ITU-T G.783 Sections 9-10
- ITU-T G.784
- ITU-T G.803
- ITU-T G.813
- ITU-T G.825
- ITU-T G.826
- ITU-T G.841
- ITU-T G.957 Table 3
- ITU-T G.958
- ITU-T I.361
- ITU-T I.363
- ITU I.432
- ITU-T Q.2110
- ITU-T Q.2130
- ITU-T Q.2140
- ITU-T Q.2931
- ITU-T O.151
- ITU-T O.171
- ETSI ETS 300 417-1-1
- TAS SC BISDN (1998)
- ACA TS 026 (1997)
- BABT /TC/139 (Draft 1e)

2524 Fls: 1a

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS Nº 03/2006 - CN
CPMI - CORREIOS
0351
Fls:
Doc: 3701

2523
Paula

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San J 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

All contents are Copyright © 1992–2002, Cisco Systems, Inc. All rights reserved. CCIP, the Cisco Arrow logo, the Cisco *Powered* Network mark, the Cisco Systems Verified logo, Cisco Unity, Follow Me Browsing, FormShare, Internet Quotient, iQ Breakthrough, iQ Expertise, iQ FastTrack, the iQ logo, iQ Net Readiness Scorecard, Networking Academy, ScriptShare, SMARTnet, TransPath, and Voice LAN are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, Discover All That's Possible, The Fastest Way to Increase Your Internet Quotient, and iQuick Study are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherSwitch, Fast Step, GigaStack, IOS, IP/TV, LightStream, MGX, MICA, the Networkers logo, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, RateMUX, Registrar, SlideCast, StrataView Plus, Stratm, SwitchProbe, TeleRouter, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0207R)

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0352
Fls:
Doc: 3701

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0353
Fls:
Doc: 3701

Cisco Systems

2522 Paula

Q & A

Firewall Services Module for the Cisco Catalyst 6500 Series Switch and Cisco 7600 Series Internet Router

Q. What is the Firewall Services Module?

A. The Firewall Services Module (FWSM) is a Catalyst 6500 Series multigigabit firewall module. The FWSM is a fabric-enabled module capable of interacting with both the bus as well as the switch fabric. The FWSM provides stateful firewall functionality in a Cisco Catalyst 6500 Series Switch and Cisco 7600 Series Internet Router.

Q. What are the key features of the FWSM?

A. Key FWSM features:

- High-performance, OC-48 or 5 Gbps throughput, full-duplex firewall functionality
- Includes entire PIX 6.0 software feature set and the following features of PIX 6.2:
  - Command authorization
  - Object grouping
  - ILS/NetMeeting fixup
  - URL filtering enhancement
- 3M pps throughput
- Support for 100 VLANs
- 1M concurrent connections
- LAN failover: active/standby, inter/intra chassis
- Dynamic Routing with OSPF/RIP
- Supports multiple modules per chassis

Q. What is the difference between the Firewall Services Module (FWSM) and the Cisco PIX® Firewall?

A. The FWSM is an integrated module for the Cisco Catalyst 6500 Series Switch and the Cisco 7600 Series Internet Router—unlike the standalone Cisco PIX® Firewall.

The FWSM is based on Cisco PIX technology.

Q. What operating system does the FWSM run?

A. The FWSM and Cisco PIX Firewall run the same operating system: Finesse, the real-time operating system. Finesse, which is a true microkernel, provides software reusability, source-code portability, increased product quality, decreased testing, shorter time to market, and increased return on investment.

Q. What mechanism does the FWSM use to inspect traffic?

A. The FWSM uses the same algorithm for inspection as the Cisco PIX Firewall: Adaptive Security Algorithm (ASA). ASA is a stateful inspection engine that inspects traffic integrity. ASA takes the source and destination addresses and ports, TCP sequence numbers, and additional TCP flags and hashes the IP header information. Hashing works like a fingerprint, creating a code that uniquely identifies the client that initiates the inbound or outbound connection.

Cisco Systems, Inc.
All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 0354
Doc: 3791

For further ASA documentation refer to:

http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_60/config/intro.htm

Q. What are the feature differences between the Cisco PIX Firewall and the FWSM?

A. The FWSM supports all Cisco PIX Firewall version 6.0 features and select version 6.2 features. The following table lists general differences. For a detailed description of differences, refer to the "Cisco PIX vs. Firewall Module Differences" document (http://www.cisco.com/en/US/products/hw/modules/ps2706/ps4452/index.html).

Q. What is the performance of the FWSM?

A. Aggregate performance is approximately 5 Gbps. The FWSM can support one million concurrent connections with a setup rate of more than 100,000 connections per second.

Q. What are some of the typical deployments for a Catalyst 6500 with FWSM?

A. Cisco Catalyst 6500 Series combined with the FWSM offers the highest performing firewall function to date—allowing corporations to collapse mission critical firewall functions into a switch chassis, reducing the number of discrete firewalls and simplifying the management of multiple firewalls. The FWSM is deployed at the enterprise campus edge and at distribution points.

A. What are the minimum software releases required for the FWSM?

A. The minimum IOS software release is Release 12.1(13)E and the minimum hybrid CatOS software release is 7.5(1)

Q. Is FWSM fabric enabled?

A. Yes. The FWSM is fabric-enabled. It has one connection to the bus and one connection to the switch fabric.

Q. Does the FWSM use Hot Standby Resource Protocol (HSRP) for redundancy?

A. No, primary and redundant FWSMs use the same protocol as the Cisco PIX Firewall for exchanging logical updates and stateful information.

Q. How is traffic sent to the FWSM? Does the module have any external ports?

A. There are no external ports on the FWSM. Some of the virtual LANs (VLANs) carrying traffic are assigned to the FWSM, and traffic on those VLANs is protected by firewalls.

Q. Does the FWSM support redundancy?

A. Stateful firewall failover is available at FCS. The FWSM is designed to work with the PIX stateful failover feature. The FWSM module can be installed in the same or a different Catalyst 6500 Series switch.

Q. Does the FWSM support Routing Protocols?

A. Yes. It supports Open Shortest Path First (OSPF) and Routing Interface Protocol (RIP).

Q. When ordering the FWSM, what product numbers should I use?

A. The product numbers for the FWSM are:

Product Number	Description
WS-SVC-FWM-1-K9	Firewall Service Module for Cisco Catalyst 6500
WS-SVC-FWM-1-K9=	Firewall Service Module for Cisco Catalyst 6500 (spare)
SC-SVC-FWM-1.1-K9	Firewall Module Software for Catalyst 6500
SC-SVC-FWM-1.1-K9=	Firewall Module Software for Catalyst 6500 (spare)

Q. Does the FWSM have any licensing options?

A. No, there are no licensing options with the module, either restricted or unrestricted.

Q. What Triple Data Encryption Standard (3DES) software does the FWSM use?

A. The encryption on the FWSM is used only for network management purposes. You cannot use the 3DES software on the module for remote access or site-to-site tunnel termination.

Q. Is 3DES software included with the module software or do I need to order it separately?

A. 3DES comes bundled with the software image. You do not have to order it separately.

Q. How much Flash and DRAM memory is available on board and can I upgrade the DRAM?

A. The Flash size on the FWSM is 128 MB and the DRAM memory is 1 GB. Memory is not field upgradable.

Q. What certifications are available for the FWSM?

A. We expect to have ICSA certifications by Q4CY02.

Q. Can I terminate remote virtual private networking (VPN) users on the FWSM?

A. No, the FWSM does not provide VPN capabilities.

Cisco Systems, Inc.
All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

ECT 2521 Paula

RQS Nº 03/2005 - CN
CRMI - CORREIOS
0355
Fls:
3701
Doc:

Q. Can I put multiple modules in the same chassis?

A. Yes, up to four modules per chassis.

Q. Does the FWSM support multicast?

A. The initial release does not support multicast, but multicast support is on the roadmap.

Q. Can I install and run the FWSN with the IPSec VPN accelerator module in the same chassis?

A. No. The IOS images for initial release are incompatible, so the modules cannot be installed in the same chassis.

Q. Does the FWSM support the IDSM Intrusion Detection module?

A. The Firewall Services Module and IDS module can coexist in the same chassis. Since the IDS module is a passive device, VLANs that are firewalled can also be spanned to the IDS module for intrusion detection.

Q. Does the FWSM provide Denial of Service/DDoS detection and management?

A. Thresholds, logging, and settings may be configured based on protocol or address.

Q. What Denial of Service attacks can the FWSM detect?

A. It detects the following attacks:

- ICMP Flood
- UDP Flood
- Ping of Death
- IP Spoofing
- IP Source Route Option

Q. Does the FWSM support the IP source route filter option?

A. IP source route filtering is provided in IOS.

Q. Can the FWSM support URL/HTTP filtering?

A. Yes, in conjunction with web filtering tools like Websense.

Q. What is the default security posture of the FWSM?

A. The FWSM denies all packets in all directions, including pings from the management interface.

Q. Does the FWSM provide high availability active/active support?

A. FWSM provides active/passive support today. Active/active is currently under investigation.

Q. Does the FWSM active/passive redundancy feature provide hitless failover?

A. Yes.

Q. Does the FWSM support traffic shaping?

A. Traffic shaping is supported via the Catalyst 6500 line cards, which provide the VLAN interfaces to the FWSM.

Q. Does the FWSM support QoS mechanisms and rate limiting?

A. Yes, it supports all Catalyst 6500 QoS capabilities.

Q. Does the FWSM support secure out-of-band management?

A. Yes, via IPSec on the management VLAN.

Q. Does FWSM support Traceroute and ping?

A. Yes, if explicitly allowed. Not supported by default.

Q. What application should be used to configure the FWSM and monitor syslog traffic?

A. At initial release, the FWSM is managed via CLI and the Cisco PIX Device Manager (PDM). PDM uses wizard-based menus to guide users through firewall configuration. For more information, visit:

http://www.cisco.com/warp/public/cc/pd/nemnsw/vpdvmn/index.shtml

In addition the FWSM is supported by Cisco AVVID partners.

Cisco Systems, Inc.
All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

2520 Paula

RE/SAN Nº 03/2005 - GN
CPMI - CORREIOS
0356
Fls:
3701
Doc:

2519
Paula

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

All contents are Copyright © 1992–2002, Cisco Systems, Inc. All rights reserved. Catalyst, Cisco, Cisco IOS, Cisco Systems, and the Cisco Systems logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0207R)

LW3514 0802

RQS N° 03/2005 - CN
CPMI - CORREIOS
0357
Fls:
3701
Doc:

RQS Nº 03/2005
CPMI - CORREIO
Fls: 0358
Doc: 3701

2517
Paula

rt 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).

9: Smart Serial Connector Cables

erface Card	Cable Type	Product Number	Length	Gender
S (up to 128 kbps Sync or 115.2 kbps	V.35 DTE	CAB-SS-V35MT(=)	10 ft (3.048 m)	Male
(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

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0359
Fls: 1
3701
Doc:

Apêndice AP

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0360
Fls:
Doc: 3701

2516 Paula

translate lat

To translate a connection request to another protocol connection type when receiving a local-area transport (LAT) request, use the **translate lat** command in global configuration mode. To remove or change the translation request, use the **no** form of this command.

translate lat *incoming-service-name* [*incoming-options*] *protocol outgoing-address* [*outgoing-options*] [*global-options*]

no translate lat *incoming-service-name* [*incoming-options*] *protocol outgoing-address* [*outgoing-options*] [*global-options*]

Syntax Description

incoming-service-name	A LAT service name. When used on the incoming portion of the command, *incoming-service-name* is the name of the service that users specify when trying to make a translated connection. This name can match the name of the final destination resource, but is not required to. This argument is useful when making remote translated connections.
incoming-options	(Optional) An incoming connection request option. For LAT, the only option currently supported is: • **unadvertised**—Prevents service advertisements from being broadcast to the network. This keyword can be useful, for example, when you define translations for many printers, and you do not want these services advertised to other LAT terminal servers. (VMS systems will be able to connect to the service even though it is not advertised.)
protocol outgoing-address	A protocol name followed by an address or host name. Protocol translation choices are: **ppp**, **slip**, **tcp**, and **x25**. **Note** The host name is resolved to an address during configuration, unless you are translating to TCP and use the **host-name** keyword, which allows the host name to be resolved at connection time instead of configuration time. See Table 38 for more information about the **host-name** keyword. Additional keywords that can be entered with the protocol are as follows: • **autocommand**—Specifies an EXEC command for an outgoing connection. The command executes upon connection to a host. You can issue any EXEC command and any switch or host name as an argument to the **autocommand** command. If the string following **autocommand** has one or more spaces as part of the string, you must place quotation marks (" ") around the string.

CPMI TR-155 0361 Fls: 3701 Doc:

	If you want to enable AppleTalk Remote Access (ARA) on an outgoing connection, specify the **autocommand arap** keywords. These keywords are necessary for ARA because ARA does not use addressing, and this option permits you to invoke the ARA string. • **virtual-template**—Associates a virtual template with a virtual access interface. See the **translate lat (virtual access interfaces)** command description for more information.
outgoing-options	(Optional) Outgoing connection request options. Choices depend upon the protocol or command entered. See Table 36, Table 37, Table 38, and Table 39 for more information.
global-options	(Optional) One or more of the following translation options can be used by any connection type: • **access-class** *number*—Allows the incoming call to be used by source hosts that match the access list parameters. The argument *number* is an integer previously assigned to an access list. Standard access list numbers are in the range from1 to 99; expanded standard access lists numbers are in the range 1300 to 1999. • **local**—Allows Telnet protocol negotiations to *not* be translated. • **login**—Requires that the user log in before the outgoing connection is made. This type of login is specified on the virtual terminal lines with the **login** command. • **max-users** *number*—Limits the number of simultaneous users of the translation to *number* (an integer you specify). • **quiet**—Suppresses printing of user-information messages.

Defaults

No default translation parameters

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.1	The **no-reset** permanent virtual circuits (PVC) subkeyword was added to support outgoing PVCs.

Usage Guidelines

You define protocol translation connections by supplying a protocol keyword and the address, host name, or service name. A LAT protocol translation command can be as simple as the following example:

```
Router(config)# translate lat LAT-1 X.25 1236672
```

However, the Cisco IOS software provides a broad range of options that support protocol translations in many networking environments. Table 36, Table 37, Table 38, and Table 39 list the **translate lat** translation options by protocol.

You can also use the Cisco IOS command-line interface to help you understand how these keywords are entered. In global configuration mode, begin entering the **translate** command and add a question mark at each portion of the command to display the options available. Some examples follow:

```
Router(config)# translate lat ?

  WORD  LAT service name

Router(config)# translate lat LSVC ?

  autocommand       Associate a command with a translation on this connections
  lat               DEC LAT protocol
  ppp               Virtual async PPP
  slip              Virtual async SLIP
  tcp               TCP/IP Telnet
  unadvertised      Prevent service advertisements from being broadcast to the
                    network
  virtual-template  Associate a virtual template with virtual access interface
  x25               X.25

Router(config)# translate lat LSVC tcp ?

  Hostname or A.B.C.D  IP address


Router(config)# translate lat LSVC tcp 1.1.1.1 ?

  access-class      Allow access list parameters to be used by source hosts
  binary            Negotiate Telnet binary mode on the connection
  host-name         Store the host name rather than its IP address
  local             Allow Telnet protocol negotiations not to be translated
  login             Require that the user log in before the outgoing connection
                    is made
  max-users         Limit the number of simultaneous users of the translation
  multibyte-IAC     Always treat multiple IACs as telnet command
  port              Port Number
  quiet             Suppress printing of user-information messages
  source-interface  Specify source interface
  stream            Treat telnet escape characters as data
```

Note If you plan to translate to X.25 on a permanent virtual circuit (PVC), see the description for the **translate x25** command for important configuration notes.

Table 36 LAT-to-PPP Outgoing Translation Options

Outgoing PPP Translation

ppp {*ip-address* | **ip-pool** [**scope-name** *name*]}

Translates from LAT to virtual asynchronous PPP. Supply an IP address as a standard, four-part dotted decimal IP address.

The **ip-pool** keyword obtains an IP address from a Dynamic Host Configuration Protocol (DHCP) proxy client or a local pool. If the optional **scope-name** keyword is not specified, the address is obtained from a DHCP proxy client. If the **scope-name** keyword is specified, the IP address is obtained from the specified local pool. The **scope-name** keyword can specify a range of IP addresses.

CPMI TR-157 CORREIOS 0362 Fls: Doc 3701

Table 36 LAT-to-PPP Outgoing Translation Options (continued)

Outgoing PPP Connection Request Options

Add any of the following keywords to configure PPP connection requests:

- **authentication** {**pap** | **chap**}—Sets Challenge Handshake Authentication Protocol (CHAP) or Password Authentication Protocol (PAP) authentication for PPP on virtual asynchronous interfaces. If you specify both keywords, order is significant; the system will try to use the first authentication type, then the second.
- **header-compression**—Implements header compression on IP packets only.
- **ipx loopback** *number*—Specifies the loopback interface to be created and permits clients running IPX-PPP to connect through virtual terminal lines on the router. A loopback interface must have been created and configured with a Novell IPX network number before IPX-PPP can work on the virtual terminal line. The virtual terminal line is assigned to the loopback interface.
- **keepalive** *number-of-seconds*—Specifies the interval at which keepalive packets are sent on Serial Line Internet Protocol (SLIP) and PPP virtual asynchronous interfaces. By default, keepalive packets are enabled and sent every 10 seconds. To shut off keepalive packets, use a value of 0. The active keepalive interval is 1 through 32,767 seconds. When you do not change from the default of 10, the keepalive interval does not appear in **more system:running-config** or **show translate** command output.
- **mtu** *bytes*—Sets the interface maximum transmission unit (MTU) of packets that the virtual asynchronous interface supports. The default MTU is 1500 bytes on a virtual asynchronous interface. The acceptable range is from 64 to 1,000,000 bytes.
- **routing**—Permits routing updates between connections. This keyword is required if the destination device is not on a subnet connected to one of the interfaces on the router.
- **use-tacacs**—Uses TACACS to verify PPP authentications for CHAP or PAP on virtual asynchronous interfaces.

Table 37 LAT-to-SLIP Outgoing Translation Options

Outgoing SLIP Translation

slip {*ip-address*| **ip-pool** [**scope-name** *name*]}

Translates from LAT to virtual asynchronous SLIP. Supply an IP address as a standard, four-part dotted decimal IP address.

The **ip-pool** keyword obtains an IP address from a DHCP proxy client or a local pool. If the optional **scope-name** keyword is not specified, the address is obtained from a DHCP proxy client. If the **scope-name** keyword is specified, the IP address is obtained from the specified local pool. The **scope-name** keyword can specify a range of IP addresses.

Note The **slip** argument applies only to outgoing connections; SLIP is not supported on incoming protocol translation connections.

2512 Paula

Table 37 LAT-to-SLIP Outgoing Translation Options (continued)

Outgoing SLIP Connection Request Options

Add any of the following keywords to configure SLIP connection requests:

- **header-compression [passive]**—Implements header compression on IP packets only. The **passive** keyword permits compression on outgoing packets only if incoming TCP packets on the same virtual asynchronous interface are compressed. The default (without the **passive** keyword) permits compression on all traffic.
- **ipx loopback** *number*—Specifies the loopback interface to be created and permits clients running IPX-PPP to connect through virtual terminal lines on the router. A loopback interface must have been created and configured with a Novell IPX network number before IPX-PPP can work on the virtual terminal line. The virtual terminal line is assigned to the loopback interface.
- **keepalive** *number-of-seconds*—Specifies the interval at which keepalive packets are sent on SLIP and PPP virtual asynchronous interfaces. By default, keepalive packets are enabled and sent every 10 seconds. To shut off keepalive packets, use a value of 0. The active keepalive interval is 1 through 32,767 seconds. When you do not change from the default of 10, the keepalive interval does not appear in **more system:running-config** or **show translate** command output.
- **mtu** *bytes*—Sets the interface MTU of packets that the virtual asynchronous interface supports. The default MTU is 1500 bytes on a virtual asynchronous interface. The acceptable range is from 64 to 1,000,000 bytes.
- **routing**—Permits routing updates between connections. This keyword is required if the destination device is not on a subnet connected to one of the interfaces on the router.

Table 38 LAT-to-TCP Outgoing Options

Outgoing TCP Translation

tcp *ip-address*

Translates LAT to TCP/IP Telnet. Supply an IP address as a standard, four-part dotted decimal IP address, the name of an IP host that can be resolved by the DNS, or explicit specification in an **ip host** command (refer to the description for the **host-name** keyword in the "Outgoing TCP Connection Request Options" section).

Outgoing TCP Connection Request Options

Any of the following optional keywords can be used to configure TCP connection requests:

- **binary**—Negotiates Telnet binary mode on the connection.
- **host-name**—Stores the host name rather than its IP address, thereby allowing the host name to be resolved at connection time instead of configuration time. There is also a **rotor** keyword suboption that you can use to modify the behavior of the **host-name** keyword by allowing one of the IP addresses defined by the **ip host** configuration command to be chosen randomly. If one address fails, another one will be tried, and so on until all address choices are exhausted. You can use the **rotor** keyword, therefore, to provide basic load sharing of the IP destinations.
- **multibyte-IAC**—Always treat multiple Interpret as Command (IAC) escape character codes as a Telnet command.
- **port** *number*—For outgoing connections, enter the number of the port to match. The default is port 23 (Telnet).

DOS nº 03/2005 - CN
CPMI TR-159 CORREIOS
Fls: 0363
Doc: 3701

Table 38 LAT-to-TCP Outgoing Options (continued)

- **source-interface** --Specifies the source address used for Telnet connections initiated by the router.
- **stream**—Performs stream processing, which enables a raw TCP stream with no Telnet control sequences. A stream connection does not process or generate any Telnet options, and also prevents Telnet processing of the data stream. This keyword might be useful for connections to ports running the UNIX-to-UNIX Copy Program (UUCP) or other non-Telnet protocols, or to ports connected to printers. For ports connected to printers using Telnet, the **stream** keyword prevents some of the problems associated with using Telnet for printers, such as unusual events happening to carriage returns or line feeds and echoing of data back to VMS systems.

Table 39 LAT-to-X.25 Outgoing Translation Options

Outgoing X.25 Translation

x25 *x.121-address*

Translates LAT to the X.25 protocol. Supply an X.121 address that conforms to the specifications provided in the *CCITT 1984 Red Book*, or the name of an X.25 host that can be resolved by the DNS, or explicit specification in an **x25 host** command.

The address number generally consists of a portion that is administered by the public data network (PDN) and a portion that is locally assigned. You must be sure that the numbers that you assign agree with the addresses assigned to you by the X.25 service provider. The X.121 addresses generally will be subaddresses of the X.121 address for the X.25 network interface.

Outgoing X.25 Connection Request Options

Any of the following optional keywords can be used to configure X.25 connection requests:

- **cud** *c-u-data*—Sends the specified X.25 Call User Data (CUD) text as part of an outgoing call request after the protocol identification bytes.
- **no-reverse**—Specifies that outgoing calls not request the X.25 reverse charge facility, when the interface default is that all outgoing calls are reverse charged.
- **profile** *profile*—Sets the X.3 packet assembler/disassembler (PAD) parameters as defined in the profile created by the **x29 profile** command.
- **pvc** *number* [**interface serial** *number* | **packetsize** *in-size out-size* | **windowsize** *in-size out-size* | **no-reset**]—Specifies that the outgoing connection is actually a PVC. The *number* argument specifies the virtual circuit channel number of the connection, which must be less than the virtual circuits assigned to the switched virtual circuit (SVC).Only one session is allowed per PVC. Use the following optional keywords to further define the connection:
  - **interface serial** *number*—Specifies a PVC interface on which to set up the PVC connection.
  - **packetsize** *in-size out-size*—Specifies the input packet size (*in-size*) and output packet size (*out-size*) for the PVC. Valid packet size values are: 16, 32, 64, 128, 256, 512, 1024, 2048, and 4096.
  - **windowsize** *in-size out-size*—Specifies the packet count for input windows (*in-size*) and output windows (*out-size*) for the outgoing translation. Values of *in-size* and *out-size* range from 1 to 127 and must not be greater than the value set for the **x25 modulo** command. You must specify the same value for *in-size* and *out-size*.
  - **no-reset**—Causes the Cisco router to send a no Reset packet request at startup of a TCP or LAT to permanent virtual circuit (PVC) translation session.

2510 Paula

Table 39 LAT-to-X.25 Outgoing Translation Options (continued)

- **reverse**—Provides reverse charging for X.25 on a per-call rather than a per-interface basis. Requests reverse charges on a specified X.121 address, even if the serial interface is not configured to request reverse charge calls.
- **use-map**—Applies **x25 map pad** command entry options (such as CUD and idle) and facilities (such as packet in, packet out, win in, and win out) to the outgoing protocol translation call. When the **use-map** keyword is specified on the **translate** command, the Destination address and optional PAD Protocol Identification (PID), CUD, and facilities are checked against a configured list of **x25 map pad** entries. If a match is found, the map entry PID, CUD, and facilities are applied to the outgoing protocol translation call. The X.25 map facilities applied to the outgoing translation can be displayed with the **show translation** command throughout the duration of the translation session.

Examples

The following example illustrates incoming LAT to outgoing TCP translations. The **unadvertised** keyword prevents broadcast of service advertisements to other servers in the network. Outgoing translated packets are sent to IP host Host1, TCP port 4005.

```
translate lat pt-printer1 unadvertised tcp Host1 port 4005
```

The following example translates LAT on an incoming line to SLIP on an outgoing line. It uses header compression only if incoming TCP packets on the same interface are compressed.

```
translate lat Service1 slip 10.0.0.4 header-compression
```

The following example first shows how to disable keepalive packets on a PPP line using the **translate lat** command, then shows translated session output from the **show translate** EXEC command indicating keepalive packets have been turned off.

```
translate lat Service2 ppp 172.21.2.2 keepalive 0
.
.
.
Router# show translate

Translate From: LAT Service2
          To:   PPP 172.21.2.2 keepalive 0
          0/0 users active, 0 peak, 0 total, 0 failures
```

Related Commands

Command	Description
show translate	Displays configured translation sessions.
translate tcp	Translates a TCP connection request automatically to another outgoing protocol connection.
translate x25	Translates an X.25 connection request automatically to another outgoing protocol connection.
x29 access-list	Limits access to the access server from certain X.25 hosts.
x29 profile	Creates a PAD profile script for use by the **translate** command.

ROS Nº 03/2005 CN
CPMI TR-161 OS
0364
Fls:
Doc: 3791

translate lat (virtual access interfaces)

When receiving a local-area transport (LAT) connection request to a service name, to set up the Cisco router to automatically translate the request to another outgoing protocol connection type, use the **translate lat** command in global configuration mode. To remove or change the translation request, use the **no** form of this command.

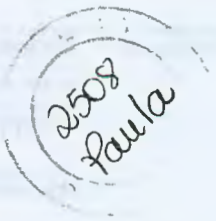
The command syntax that follows shows how to apply a virtual interface template in place of outgoing **translate** options. If you are using virtual templates for protocol translation, all outgoing options are defined in the virtual interface template. Table 40 lists all outgoing options and their corresponding interface configuration commands.

translate lat *incoming-service-name* [*incoming-options*] **virtual-template** *number* [*global-options*]

no translate lat *incoming-service-name* [*incoming-options*] **virtual-template** *number* [*global-options*]

Syntax Description

incoming-service-name	A LAT service name. When used on the incoming portion of the **translate lat** command, *service-name* is the name of the service that users specify when trying to make a translated connection. This name can match the name of the final destination resource, but this match is not required. Such matches can be useful when making remote translated connections.
incoming-options	(Optional) An incoming connection request option. For LAT, the only keyword currently supported is: • **unadvertised**—Prevents service advertisements from being broadcast to the network. This keyword can be useful, for example, when you define translations for many printers, and you do not want these services advertised to other LAT terminal servers. (VMS systems will be able to connect to the service even though it is not advertised.)
virtual-template *number*	Applies the virtual interface template specified by the *number* argument in place of outgoing options.
global-options	(Optional) Translation options that can be used by any connection type and can be one or more of the following: • **access-class** *number*—Allows the incoming call to be used by source hosts that match the access list parameters. The argument *number* is an integer previously assigned to an access list. Standard access list numbers are in the range from1 to 99; expanded standard access lists numbers are in the range 1300 to 1999. • **max-users** *number*—Limits the number of simultaneous users of the translation to *number* (an integer you specify). • **local**—Allows Telnet protocol negotiations to *not* be translated. • **login**—Requires that the user log in before the outgoing connection is made. This type of login is specified on the virtual terminal lines with the **login** command. • **quiet**—Suppresses printing of user-information messages.



Defaults

No default translation parameters

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

You define the protocol translation connections by choosing a protocol keyword and supplying the appropriate address, host name, or service name. The protocol connection information is followed by optional features for that connection, as appropriate. For example, the **binary** keyword is only appropriate with TCP/IP connections. The global options, in general, apply to all the connection types, but there are exceptions.

Rather than specifying outgoing translation options in the **translate** command, configure these options as interface configuration commands under the virtual interface template, then apply the virtual interface template to the **translate** command. Table 40 maps outgoing **translate** command options to interface commands you can configure in the virtual interface template.

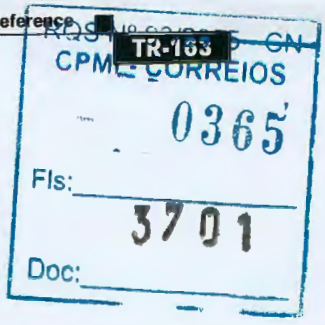
Table 40 Mapping Outgoing translate lat Options to Interface Commands

translate lat Command Options	Corresponding Interface Configuration Command
ip-pool	**peer default ip address** {**ip-address** | **dhcp** | **pool** [*poolname*]}
header-compression	**ip tcp header compression** [**on** | **off** | **passive**]
routing	**ip routing** or **ipx routing**
mtu	**mtu**
keepalive	**keepalive**
authentication {**chap** | **pap**}	**ppp authentication** {**chap** | **pap**}
ppp use-tacacs	**ppp use-tacacs**
ipx loopback	**ipx ppp-client loopback** *number*

Examples

The following example configures PPP tunneling from a PC across a LAT network. The remote PC is given the IP address 10.12.118.12 when it dials in. The **unadvertised** keyword prevents broadcast of service advertisements to other servers.

```
interface Virtual-Template1
 ip unnumbered Ethernet0
 peer default ip address 10.12.118.12
 ppp authentication chap
!
translate lat pt-printer1 unadvertised virtual-template 1
```

Related Commands

Command	Description
show translate	Displays configured translation sessions.
translate tcp	Translates a TCP connection request automatically to another outgoing protocol connection.
translate x25	Translates an X.25 connection request automatically to another outgoing protocol connection.
x29 access-list	Limits access to the access server from certain X.25 hosts.
x29 profile	Creates a PAD profile script for use by the **translate** command.

2506 Paula

translate tcp

To translate a connection request to another protocol connection type when receiving a TCP connection request to a particular destination address or host name, use the **translate tcp** command in global configuration mode. To remove or change the translation request, use the **no** form of this command.

translate tcp *incoming-address* [*incoming-options*] *protocol outgoing-address* [*outgoing-options*] [*global-options*]

no translate tcp *incoming-address* [*incoming-options*] *protocol outgoing-address* [*outgoing-options*] [*global-options*]

Syntax Description

incoming-address	Standard IP address in standard, four-part dotted decimal notation. The IP address cannot be in use by other routers, and it should be on a connected subnet.
incoming-options	(Optional) An incoming connection request option. Choices are as follows: • **binary**—Negotiates Telnet binary mode on the Telnet connection. (This was the default in previous versions of the protocol translation software and is set automatically when you enter a **translate** command in the previous format.) • **port** *number*—The number of the port to match for incoming connections. The default is port 23 (Telnet). For outgoing connections, enter the number of the port to use. The default is port 23. • **printer**—Supports local-area transport (LAT) and X.25 printing over a TCP network among multiple sites. This keyword causes the protocol translation software to delay the completion of an incoming Telnet connection until after the outgoing protocol connection (to LAT or X.25) has been successfully established. An unsuccessful outgoing connection attempt results in the TCP connection to the router being refused, rather than being accepted and then closed, which is the default behavior. Note that using this keyword will force the global **quiet** keyword to be applied to the translation. • **stream**—Performs stream processing, which enables a raw TCP stream with no Telnet control sequences. A stream connection does not process or generate any Telnet options, and also prevents Telnet processing of the data stream. This keyword might be useful for connections to ports running the UNIX-to-UNIX Copy Program (UUCP) or other non-Telnet protocols, or to ports connected to printers. For ports connected to printers using Telnet, the **stream** keyword prevents some of the problems associated with using Telnet for printers, such as unusual events happening to carriage returns or line feeds and echoing of data back to VMS systems.

TR-165
CORREIOS
0366
Fls:
Doc: 3701

protocol outgoing-address	A protocol name followed by an address or host name. Protocol translation choices are: **lat**, **ppp**, **slip**, and **x25**. Additional keywords that can be entered with the protocol are as follows: • **autocommand**—Specifies an EXEC command for an outgoing connection. The command executes upon connection to a host. You can issue any EXEC command and any switch or host name as an argument to the **autocommand** keyword. If the string following **autocommand** has one or more spaces as part of the string, you must place quotation marks (" ") around the string. If you want to enable AppleTalk Remote Access (ARA) on an outgoing connection, specify the **autocommand arap** keywords. These keywords are necessary for ARA because ARA does not use addressing, and this option permits you to invoke the ARA string. • **virtual-template**—Associates a virtual template with a virtual access interface. See the **translate tcp (virtual access interfaces)** command description for more information.
outgoing-options	(Optional) Outgoing connection request options. Choices depend upon the protocol or command entered. See Table 41, Table 42, Table 43, and Table 44 for more information.
global-options	(Optional) One or more of the following translation options can be used by any connection type: • **access-class** *number*—Allows the incoming call to be used by source hosts that match the access list parameters. The argument *number* is an integer previously assigned to an access list. Standard access list numbers are in the range from1 to 99; expanded standard access lists numbers are in the range 1300 to 1999. • **local**—Allows Telnet protocol negotiations to *not* be translated. • **login**—Requires that the user log in before the outgoing connection is made. This type of login is specified on the virtual terminal lines with the **login** command. • **max-users** *number*—Limits the number of simultaneous users of the translation to *number* (an integer you specify). • **quiet**—Suppresses printing of user-information messages. • **swap**—Valid for TCP-to-X.25 translations only, and allows X.3 parameters to be set on the router by the host originating the X.25 call, or by an X.29 profile. This configuration enables incoming and outgoing X.25 connections to be swapped so that the device is treated like a PAD when it accepts a call. By default, the router functions like a PAD for calls that it initiates, and like an X.25 host for calls it accepts. The **swap** keyword allows connections from an X.25 host that wants to connect to the router, and then treats it like a PAD.

Defaults No default translation parameters

Command Modes Global configuration

2504 Paula

Command History

Release	Modification
10.0	This command was introduced.
12.1	The **no-reset** permanent virtual circuits (PVCs) subkeyword was added to support outgoing PVCs.

Usage Guidelines

You define protocol translation connections by supplying a protocol keyword and the address, host name, or service name. A TCP protocol translation command can be as simple as the following example:

```
Router(config)# translate tcp 10.1.1.1 X.25 1236672
```

However, the Cisco IOS software provides a broad range of options that support protocol translations in many networking environments. Table 41, Table 42, Table 43, and Table 44 list the **translate tcp** translation options by protocol.

You can also use the Cisco IOS command-line interface to help you understand how these keywords are entered. In global configuration mode, begin entering the **translate** command and add a question mark at each portion of the command to display the options available. Some examples follow:

```
Router(config)# translate tcp ?

  Hostname or A.B.C.D  IP address

Router(config)# translate tcp 1.1.1.1 ?

  autocommand       Associate a command with a translation on this connections
  binary            Negotiate Telnet binary mode on the connection
  lat               DEC LAT protocol
  port              Port Number
  ppp               Virtual async PPP
  printer           Enable non-interactive (implies global quiet)
  slip              Virtual async SLIP
  stream            Enable stream processing
  tcp               TCP/IP Telnet
  virtual-template  Associate a virtual template with virtual access interface
  x25               X.25

Router(config)# translate tcp 1.1.1.1 lat LAT-1 ?

  access-class  Allow access list parameters to be used by source hosts
  local         Allow Telnet protocol negotiations not to be translated
  login         Require that the user log in before the outgoing connection is
                made
  max-users     Limit the number of simultaneous users of the translation
  node          LAT node name
  port          LAT port name
  quiet         Suppress printing of user-information messages
  unadvertised  Prevent service advertisements from being broadcast to the
                network
```

Note If you plan to translate to X.25 on a permanent virtual circuit (PVC), see the description for the **translate x25** command for important configuration notes.

TR-157
CPMI - CORREIOS
0367
Fls:
3701
Doc:

Table 41 TCP-to-LAT Outgoing Options

Outgoing LAT Translation

lat *service-name*

Translates TCP to the LAT protocol.The software must learn the service name through LAT service advertisements before it can use the service.

Outgoing LAT Connection Request Options

Any of the following optional keywords can be used to configure LAT connection requests:

- **node** *name*—Connects to the specified node that offers a LAT service. By default, the connection is made to the highest-rated node that offers the service.
- **port** *name*—Destination LAT port name in the format of the remote system. This parameter is usually ignored in most time-sharing systems, but is used by terminal servers that offer reverse-LAT services.
- **unadvertised**—Prevents LAT service advertisements from being broadcast to the network.

Table 42 TCP-to-PPP Outgoing Options

Outgoing PPP Translation

ppp {*ip-address* / **ip-pool** [**scope-name** *name*]}

Translates from TCP to virtual asynchronous PPP. Supply an IP address as a standard, four-part dotted decimal IP address.

The **ip-pool** keyword obtains an IP address from a Dynamic Host Configuration Protocol (DHCP) proxy client or a local pool. If the **scope-name** keyword is not specified, the address is obtained from a DHCP proxy client. If the **scope-name** keyword is specified, the IP address is obtained from the specified local pool. The **scope-name** keyword can specify a range of IP addresses.

Outgoing PPP Connection Request Options

Any of the following optional keywords can be used to configure PPP connection requests:

- **authentication** {**pap** | **chap**}—Sets Challenge Handshake Authentication Protocol (CHAP) or Password Authentication Protocol (PAP) authentication for PPP on virtual asynchronous interfaces. If you specify both keywords, order is significant; the system will try to use the first authentication type, then the second.
- **header-compression** [**passive**]—Implements header compression on IP packets only. The **passive** keyword permits compression on outgoing packets only if incoming TCP packets on the same virtual asynchronous interface are compressed. The default (without the **passive** keyword) permits compression on all traffic.
- **ipx loopback** *number*—Specifies the loopback interface to be created and permits clients running IPX-PPP to connect through virtual terminal lines on the router. A loopback interface must have been created and configured with a Novell IPX network number before IPX-PPP can work on the virtual terminal line. The virtual terminal line is assigned to the loopback interface.
- **keepalive** *number-of-seconds*—Specifies the interval at which keepalive packets are sent on Serial Line Internet Protocol (SLIP) and PPP virtual asynchronous interfaces. By default, keepalive packets are enabled and sent every 10 seconds. To shut off keepalive packets, use a value of 0. The active keepalive interval is 1 through 32,767 seconds. When you do not change from the default of 10, the keepalive interval does not appear in **more system:running-config** or **show translate** command output.

2502 Paulo

Table 42 TCP-to-PPP Outgoing Options (continued)

- **mtu** *bytes*—Sets the interface maximum transmission unit (MTU) of packets that the virtual asynchronous interface supports. The default MTU is 1500 bytes on a virtual asynchronous interface. The acceptable range is from 64 to 1,000,000 bytes.
- **routing**—Permits routing updates between connections. This keyword is required if the destination device is not on a subnet connected to one of the interfaces on the router.
- **use-tacacs**—Uses TACACS to verify PPP authentications for CHAP or PAP on virtual asynchronous interfaces.

Table 43 TCP-to-SLIP Outgoing Options

Outgoing SLIP Translation

slip {*ip-address* | **ip-pool** [**scope-name** *name*]}

Translates from TCP to virtual asynchronous SLIP. Supply an IP address as a standard, four-part dotted decimal IP address.

The **ip-pool** keyword obtains an IP address from a DHCP proxy client or a local pool. If the optional **scope-name** keyword is not specified, the address is obtained from a DHCP proxy client. If the **scope-name** keyword is specified, the IP address is obtained from the specified local pool. The **scope-name** keyword can specify a range of IP addresses.

Note The **slip** keyword applies only to outgoing connections; SLIP is not supported on incoming protocol translation connections.

Outgoing SLIP Connection Request Options

Any of the following optional keywords can be used to configure SLIP connection requests:

- **header-compression [passive]**—Implements header compression on IP packets only. The **passive** keyword permits compression on outgoing packets only if incoming TCP packets on the same virtual asynchronous interface are compressed. The default (without the **passive** keyword) permits compression on all traffic.
- **ipx loopback** *number*—Specifies the loopback interface to be created and permits clients running IPX-PPP over X.25 to connect through virtual terminal lines on the router. A loopback interface must have been created and configured with a Novell IPX network number before IPX-PPP can work on the virtual terminal line. The virtual terminal line is assigned to the loopback interface.
- **keepalive** *number-of-seconds*—Specifies the interval at which keepalive packets are sent on SLIP and PPP virtual asynchronous interfaces. By default, keepalive packets are enabled and sent every 10 seconds. To shut off keepalive packets, use a value of 0. The active keepalive interval is 1 through 32,767 seconds. When you do not change from the default of 10, the keepalive interval does not appear in **more system:running-config** or **show translate** command output.
- **mtu** *bytes*—Sets the interface MTU of packets that the virtual asynchronous interface supports. The default MTU is 1500 bytes on a virtual asynchronous interface. The acceptable range is from 64 to 1,000,000 bytes.
- **routing**—Permits routing updates between connections. This keyword is required if the destination device is not on a subnet connected to one of the interfaces on the router.

RQS N TR-100 CN
CPMI - CORREIOS
0368
Fls: 3701
Doc:

Table 44 TCP-to-X.25 Outgoing Options

Outgoing X.25 Translation

x25 *x.121-address*

Translates TCP to the X.25 protocol. Supply an X.121 address that conforms to the specifications provided in the *CCITT 1984 Red Book*, or the name of an X.25 host that can be resolved by the DNS, or explicit specification in an **x25 host** command.

The address number generally consists of a portion that is administered by the public data network (PDN) and a portion that is locally assigned. You must be sure that the numbers that you assign agree with the addresses assigned to you by the X.25 service provider. The X.121 addresses generally will be subaddresses of the X.121 address for the X.25 network interface.

Outgoing X.25 Connection Request Options

Any of the following optional keywords can be used to configure X.25 connection requests:

- **cud** *c-u-data*—Sends the specified X.25 Call User Data (CUD) text as part of an outgoing call request after the protocol identification bytes.
- **no-reverse**—Specifies that outgoing calls not request the X.25 reverse charge facility, when the interface default is that all outgoing calls are reverse charged.
- **profile** *profile*—Sets the X.3 packet assembler/disassembler (PAD) parameters as defined in the profile created by the **x29 profile** command.
- **pvc** *number* [**interface serial** *number* | **packetsize** *in-size out-size* | **windowsize** *in-size out-size* | **no-reset**]—Specifies that the outgoing connection is actually a PVC. The *number* argument specifies the virtual circuit channel number of the incoming connection, which must be less than the virtual circuits assigned to the switched virtual circuit (SVC).Only one session is allowed per PVC. Use the following optional keywords to further define the connection:
  - **interface serial** *number*—Specifies a PVC interface on which to set up the PVC connection.
  - **packetsize** *in-size out-size*—Specifies the input packet size (*in-size*) and output packet size (*out-size*) for the PVC. Valid packet size values are: 16, 32, 64, 128, 256, 512, 1024, 2048, and 4096.
  - **windowsize** *in-size out-size*—Specifies the packet count for input windows (*in-size*) and output windows (*out-size*) for the outgoing translation. Values of *in-size* and *out-size* range from 1 to 127 and must not be greater than the value set for the **x25 modulo** command. You must specify the same value for *in-size* and *out-size*.
  - **no-reset**—Causes the Cisco router to send a no Reset packet request at startup of a TCP or LAT to PVC translation session.
- **reverse**—Provides reverse charging for X.25 on a per-call rather than a per-interface basis. Requests reverse charges on a specified X.121 address, even if the serial interface is not configured to request reverse charge calls.
- **use-map**—Applies **x25 map pad** command entry options (such as CUD and idle) and facilities (such as packet in, packet out, win in, and win out) to the outgoing protocol translation call. When the **use-map** keyword is specified on the **translate** command, the Destination address and optional PAD Protocol Identification (PID), CUD, and facilities are checked against a configured list of **x25 map pad** command entries. If a match is found, the map entry PID, CUD, and facilities are applied to the outgoing protocol translation call. The X.25 map facilities applied to the outgoing translation can be displayed with the **show translation** command throughout the duration of the translation session.

2500 Paula

Examples

The following example illustrates the use of the TCP incoming protocol **printer** keyword for an incoming TCP connection:

```
translate tcp 172.19.32.250 printer x25 5678
```

The following example permits clients running IPX-PPP to connect through the device virtual terminal lines to a server running PPP:

```
interface loopback0
  no ip address
  ipx network 544
  ipx sap-interval 2000
!
translate tcp 172.21.14.67 port 1234 ppp 10.0.0.2 ipx loopback0
```

Related Commands

Command	Description
show translate	Displays configured translation sessions.
translate lat	Translates a LAT connection request automatically to another outgoing protocol connection.
translate x25	Translates an X.25 connection request automatically to another outgoing protocol connection.
x29 access-list	Limits access to the access server from certain X.25 hosts.
x29 profile	Creates a PAD profile script for use by the **translate** command.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
TR-171
0369
Fls:
Doc: 3701

translate tcp (virtual access interfaces)

When receiving a TCP connection request to a particular destination address or host name, to set up the Cisco router to automatically translate the request to another outgoing protocol connection type, use the **translate tcp** command in global configuration mode. To remove or change the translation request, use the **no** form of this command.

The command syntax that follows shows how to apply a virtual interface template in place of outgoing **translate** options. If you are using virtual templates for protocol translation, all outgoing options are defined in the virtual interface template.

translate tcp *incoming-address* [*incoming-options*] **virtual-template** *number* [*global-options*]

no translate tcp *incoming-address* [*incoming-options*] **virtual-template** *number* [*global-options*]

Syntax Description

incoming-address	TCP/IP Telnet and a standard IP address or host name. The *ip-address* argument is a standard, four-part dotted decimal IP address or the name of an IP host that can be resolved by the Domain Name System (DNS) or explicit specification in an **ip host** command.
incoming-options	(Optional) Incoming connection request options. These arguments can have the following values: • **binary**—Negotiates Telnet binary mode on the Telnet connection. (This was the default in previous versions of the Cisco IOS software and is set automatically when you enter a **translate** command in the old format.) • **port** *number*—For incoming connections, enter the number of the port to match. The default is port 23 (Telnet). For outgoing connections, enter the number of the port to use. The default is port 23. • **printer**—Supports LAT and X.25 printing over a TCP network among multiple sites. This keyword causes the protocol translation software to delay the completion of an incoming Telnet connection until after the outgoing protocol connection (to LAT or X.25) has been successfully established. An unsuccessful outgoing connection attempt results in the TCP connection to the router being refused, rather than being accepted and then closed, which is the default behavior. Note that using this keyword will force the global **quiet** keyword to be applied to the translation. • **stream**—Performs stream processing, which enables a raw TCP stream with no Telnet control sequences. A stream connection does not process or generate any Telnet options, and also prevents Telnet processing of the data stream. This keyword might be useful for connections to ports running the UNIX-to-UNIX Copy Program (UUCP) or other non-Telnet protocols, or to ports connected to printers. For ports connected to printers using Telnet, the **stream** keyword prevents some of the problems associated with using Telnet for printers, such as unusual events happening to carriage returns or line feeds and echoing of data back to VMS systems.
virtual-template *number*	Applies the virtual interface template specified by the *number* argument in place of outgoing options.

2498 fls

global-options	(Optional) One or more of the following translation options can be used by any connection type: • **access-class** *number*—Allows the incoming call to be used by source hosts that match the access list parameters. The argument *number* is an integer previously assigned to an access list. Standard access list numbers are in the range from1 to 99; expanded standard access lists numbers are in the range 1300 to 1999. • **local**—Allows Telnet protocol negotiations to *not* be translated. • **login**—Requires that the user log in before the outgoing connection is made. This type of login is specified on the virtual terminal lines with the **login** command. • **max-users** *number*—Maximum number of simultaneous users of the translation. • **quiet**—Suppresses printing of user-information messages. • **swap**—Valid for TCP-to-X.25 translations only, and allows X.3 parameters to be set on the router by the host originating the X.25 call, or by an X.29 profile. This configuration enables incoming and outgoing X.25 connections to be swapped so that the device is treated like a PAD when it accepts a call. By default, the router functions like a PAD for calls that it initiates, and like an X.25 host for calls it accepts. The **swap** keyword allows connections from an X.25 host that wants to connect to the router, and then treats it like a PAD.

Defaults

No default translation parameters

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

You define the protocol translation connections by choosing a protocol keyword and supplying the appropriate address, host name, or service name. The protocol connection information is followed by optional features for that connection, as appropriate. For example, the **binary** keyword is only appropriate with TCP/IP connections. The global options, in general, apply to all the connection types, but there are exceptions.

Examples

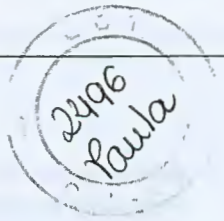
The following example illustrates the use of the TCP incoming **printer** keyword for an incoming TCP connection:

```
interface Virtual-Template1
 ip unnumbered Ethernet0
 peer default ip address 10.12.108.1
 ppp authentication chap

translate tcp 172.19.32.250 printer Virtual-Template1
```


ROS N° TR-173 - CN
CPMI - CORREIOS
0370
Fls:
Doc: 3701

Related Commands

Command	Description
show translate	Displays configured translation sessions.
translate tcp	Translates a TCP connection request automatically to another outgoing protocol connection.
translate x25	Translates an X.25 connection request automatically to another outgoing protocol connection.
x29 access-list	Limits access to the access server from certain X.25 hosts.
x29 profile	Creates a PAD profile script for use by the **translate** command.



translate x25

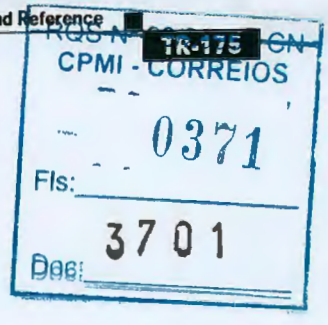
To translate a connection request to another protocol connection type when receiving an X.25 connection request to a particular destination address or host name, use the **translate x25** command in global configuration mode. To remove or change the translation request, use the **no** form of this command.

translate x25 *incoming-address* [*incoming-options* [**pvc** *number* [*pvc-options*]]] *protocol outgoing-address* [*outgoing-options*] [*global-options*]

no translate x25 *incoming-address* [*incoming-options* [**pvc** *number* [*pvc-options*]]] *protocol outgoing-address* [*outgoing-options*] [*global-options*]

Syntax Description

incoming-address	An X.25 and X.121 address that conform to specifications provided in the *CCITT 1984 Red Book*. This address generally consists of a portion that is administered by the PDN and a portion that is locally assigned. You must be sure that the numbers that you assign agree with the addresses assigned to you by the X.25 service provider. The X.121 addresses generally will be subaddresses of the X.121 address for the X.25 network interface. Typically, the interface address will be a 12-digit number. Any additional digits are interpreted as a subaddress. The PDN still routes these calls to the interface, and the Cisco IOS software is responsible for interpreting the extra digits. Do not use the same address on the interface and for translation.
incoming-options	(Optional) An incoming connection request option. Choices are as follows: • **accept-reverse**—Accepts reverse charged calls on an X.121 address even if the serial interface is not configured to accept reverse charged calls. • **cud** *c-u-data*—Specifies the Call User Data (CUD) field to match in the X.25 Incoming Call packet. If not configured, the CUD in the Incoming Call packet must be blank. • **idle** *minutes*—Specifies the number of minutes the virtual circuit is idle. This keyword enables the protocol translation function to clear a switched virtual circuit after a set period of inactivity, where *minutes* is the number of minutes in the period. Calls either originated or terminated are cleared. The maximum value of *minutes* is 255. The default value of *minutes* is zero. • **printer**—Supports local-area transport (LAT) and TCP printing over an X.25 network among multiple sites. Provides an "interlock mechanism" between the acceptance of an incoming X.25 connection and the opening of an outgoing LAT or TCP connection. This keyword causes the Cisco IOS software to delay the call confirmation of an incoming X.25 call request until after the outgoing protocol connection (to TCP or LAT) has been successfully established. An unsuccessful outgoing connection attempt to the router results in the incoming X.25 connection being refused, rather than being accepted and then closed, which is the default behavior. Note that using this keyword will force the global **quiet** keyword to be applied to the translation.



- **profile** *profile*—Sets the X.3 packet assembler/disassembler (PAD) parameters as defined in the profile created by the **x29 profile** command.
- **pvc** *number* [**interface serial** *number* | **packetsize** *in-size out-size* | **windowsize** *in-size out-size*]—Specifies that the outgoing connection is actually a PVC. The *number* argument specifies the virtual circuit channel number of the connection, which must be less than the virtual circuits assigned to the switched virtual circuit (SVC).Only one session is allowed per PVC. Use the following optional keywords to further define the connection:
  - **interface serial** *number*—Specifies a PVC interface on which to set up the PVC connection.
  - **packetsize** *in-size out-size*—Specifies the input packet size (*in-size*) and output packet size (*out-size*) for the PVC. Valid packet size values are as follows: 16, 32, 64, 128, 256, 512, 1024, 2048, and 4096.
  - **windowsize** *in-size out-size*—Specifies the packet count for input windows (*in-size*) and output windows (*out-size*) for the outgoing translation. Values of *in-size* and *out-size* range from 1 to 127 and must not be greater than the value set for the **x25 modulo** command. You must specify the same value for *in-size* and *out-size*.

protocol outgoing-address

A protocol name followed by an address or host name. Protocol translation choices are **lat**, **ppp**, **slip**, and **tcp**.

Note The host name is translated to an address during configuration, unless you are translating to TCP and use the **host-name** keyword, which allows the host name to be resolved at connection time instead of configuration time. See Table 48 for more information about the **host-name** keyword.

Additional keywords that can be entered with the protocol are as follows:

- **autocommand**—Specifies an EXEC command for an outgoing connection. The command executes upon connection to a host. You can issue any EXEC command and any switch or host name as an argument to the **autocommand** keyword. If the string following **autocommand** has one or more spaces as part of the string, you must place quotation marks (" ") around the string. If you want to enable AppleTalk Remote Access (ARA) on an outgoing connection, specify the **autocommand arap** keywords. These keywords are necessary for ARA because ARA does not use addressing, and this option permits you to invoke the ARA string.
- **virtual-template**—Associates a virtual template with a virtual access interface. See the **translate x25 (virtual access interfaces)** command description for more information.

outgoing-options	(Optional) Outgoing connection request option. Choices depend upon the protocol or command entered. See Table 45,Table 46, Table 47, and Table 48 for a list of outgoing protocol translation options.
global-options	(Optional) One or more of the following translation options can be used by any connection type: • **access-class** *number*—Allows the incoming call to be used by source hosts that match the access list parameters. The argument *number* is an integer previously assigned to an access list. Standard access list numbers are in the range from1 to 99; expanded standard access lists numbers are in the range 1300 to 1999. • **local**—Allows Telnet protocol negotiations to *not* be translated. • **login**—Requires that the user log in before the outgoing connection is made. This type of login is specified on the virtual terminal lines with the **login** command. • **max-users** *number*—Limits the number of simultaneous users of the translation to *number* (an integer you specify). • **quiet**—Suppresses printing of user-information messages. • **swap**—Valid for X.25-to-TCP translations only, and allows X.3 parameters to be set on the router by the host originating the X.25 call, or by an X.29 profile. This configuration enables incoming and outgoing X.25 connections to be swapped so that the device is treated like a PAD when it accepts a call. By default, the router functions like a PAD for calls that it initiates, and like an X.25 host for calls it accepts. The **swap** keyword allows connections from an X.25 host that wants to connect to the router, and then treats it like a PAD.

Defaults

No default translation parameters.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

You define protocol translation connections by supplying a protocol keyword and the address, host name, or service name. An X.25 protocol translation command can be as simple as the following example:

```
Router(config)# translate X.25 1236672 tcp 1.1.1.1
```

However, the Cisco IOS software provides a broad range of options that support protocol translations in many networking environments. Table 45, Table 46, Table 47, and Table 48 lists the **translate x25** translation options by protocol.

CPMI - CORREIOS
0372
Fls:
3701
Doc:

You can also use the Cisco IOS command-line interface to help you understand how these keywords are entered. In global configuration mode, begin entering the **translate** command and add a question mark at each portion of the command to display the options available. Some examples follow:

```
Router(config)# translate x25 ?

  WORD  X.121 Address pattern

Router(config)# translate x25 66666 ?

  accept-reverse    Accept reverse charge on a per-call basis
  autocommand       Associate a command with a translation on this connections
  cud               Specify the Call User Data (CUD)
  idle              Specify VC idle timer
  lat               DEC LAT protocol
  ppp               Virtual async PPP
  printer           Enable non-interactive (implies global quiet)
  profile           Use a defined X.3 profile
  pvc               An incoming connection is actually a PVC
  slip              Virtual async SLIP
  tcp               TCP/IP Telnet
  virtual-template  Associate a virtual template with virtual access interface
  x25               X.25

Router(config)# translate x25 66666 tcp 1.1.1.1 ?

  access-class      Allow access list parameters to be used by source hosts
  binary            Negotiate Telnet binary mode on the connection
  host-name         Store the host name rather than its IP address
  local             Allow Telnet protocol negotiations not to be translated
  login             Require that the user log in before the outgoing connection
                    is made
  max-users         Limit the number of simultaneous users of the translation
  multibyte-IAC     Always treat multiple IACs as telnet command
  port              Port Number
  quiet             Suppress printing of user-information messages
  source-interface  Specify source interface
  stream            Treat telnet escape characters as data
  swap              Allow X.3 parameters to be set on the protocol translator
                    by the host originating the X.25 call
```

Table 45 X.25-to-LAT Outgoing Options

Outgoing LAT Translation

lat *service-name*

Translates X.25 to the LAT protocol.The software must learn the service name through LAT service advertisements before it can use the service.

Outgoing LAT Connection Request Options

Any of the following optional keywords can be used to configure LAT connection requests:

- **node** *name*—Connects to the specified node that offers a LAT service. By default, the connection is made to the highest-rated node that offers the service.
- **port** *name*—Destination LAT port name in the format of the remote system. This parameter is usually ignored in most time-sharing systems, but is used by terminal servers that offer reverse-LAT services.
- **unadvertised**—Prevents LAT service advertisements from being broadcast to the network.

Table 46 X.25-to-PPP Outgoing Options

Outgoing PPP Translation

ppp {*ip-address* / **ip-pool** [**scope-name** *name*]}

Translates from X.25 to virtual asynchronous PPP. Supply an IP address as a standard, four-part dotted decimal IP address.

The **ip-pool** keyword obtains an IP address from a Dynamic Host Configuration Protocol (DHCP) proxy client or a local pool. If the optional **scope-name** keyword is not specified, the address is obtained from a DHCP proxy client. If the **scope-name** keyword is specified, the IP address is obtained from the specified local pool. The **scope-name** keyword can specify a range of IP addresses.

Outgoing PPP Connection Request Options

Any of the following optional keywords can be used to configure PPP connection requests:

- **authentication** {**pap** | **chap**}—Sets Challenge Handshake Authentication Protocol (CHAP) or Password Authentication Protocol (PAP) authentication for PPP on virtual asynchronous interfaces. If you specify both options, order is significant; the system will try to use the first authentication type, then the second.
- **header-compression**—Configures header compression on IP packets only.
- **ipx loopback** *number*—Specifies the loopback interface to be created and permits clients running IPX-PPP over X.25 to connect through virtual terminal lines on the router. A loopback interface must have been created and configured with a Novell IPX network number before IPX-PPP can work on the virtual terminal line. The virtual terminal line is assigned to the loopback interface.
- **keepalive** *number-of-seconds*—Specifies the interval at which keepalive packets are sent on Serial Line Internet Protocol (SLIP) and PPP virtual asynchronous interfaces. By default, keepalive packets are enabled and sent every 10 seconds. To shut off keepalive packets, use a value of 0. The active keepalive interval is 1 through 32,767 seconds. When you do not change from the default of 10, the keepalive interval does not appear in **more system:running-config** or **show translate** command output.
- **mtu** *bytes*—Sets the interface MTU of packets that the virtual asynchronous interface supports. The default MTU is 1500 bytes on a virtual asynchronous interface. The acceptable range is from 64 to 1,000,000 bytes.
- **routing**—Permits routing updates between connections. This option is required if the destination device is not on a subnet connected to one of the interfaces on the router.
- **use-tacacs**—Uses TACACS to verify PPP authentications for CHAP or PAP on virtual asynchronous interfaces.

2492 Paula
ROS Nº 03/2005 - CN
CPMI - TR-179 - OS
0373
Fls:
Doc: 3701

Table 47 X.25-to-SLIP Outgoing Options

Outgoing SLIP Translation

slip {*ip-address* / **ip-pool** [**scope-name** *name*]}

Translates from X.25 to virtual asynchronous SLIP. Supply an IP address as a standard, four-part dotted decimal IP address.

The **ip-pool** keyword obtains an IP address from a DHCP proxy client or a local pool. If the optional **scope-name** keyword is not specified, the address is obtained from a DHCP proxy client. If the **scope-name** keyword is specified, the IP address is obtained from the specified local pool. The **scope-name** keyword can specify a range of IP addresses.

Note The **slip** argument applies only to outgoing connections; SLIP is not supported on incoming protocol translation connections.

Outgoing SLIP Connection Request Options

Any of the following optional keywords can be used to configure SLIP connection requests:

- **header-compression [passive]**—Implements header compression on IP packets only. The **passive** keyword permits compression on outgoing packets only if incoming TCP packets on the same virtual asynchronous interface are compressed. The default (without the **passive** keyword) permits compression on all traffic.
- **ipx loopback** *number*—Specifies the loopback interface to be created and permits clients running IPX-PPP over X.25 to connect through virtual terminal lines on the router. A loopback interface must have been created and configured with a Novell IPX network number before IPX-PPP can work on the virtual terminal line. The virtual terminal line is assigned to the loopback interface.
- **keepalive** *number-of-seconds*—Specifies the interval at which keepalive packets are sent on SLIP and PPP virtual asynchronous interfaces. By default, keepalive packets are enabled and sent every 10 seconds. To shut off keepalive packets, use a value of 0. The active keepalive interval is 1 through 32,767 seconds. When you do not change from the default of 10, the keepalive interval does not appear in **more system:running-config** or **show translate** command output.
- **mtu** *bytes*—Sets the interface MTU of packets that the virtual asynchronous interface supports. The default MTU is 1500 bytes on a virtual asynchronous interface. The acceptable range is from 64 to 1,000,000 bytes.
- **routing**—Permits routing updates between connections. This keyword is required if the destination device is not on a subnet connected to one of the interfaces on the router.

Table 48 X.25-to-TCP Outgoing Options

Outgoing TCP Translation

tcp *ip-address*

Translates X.25 to TCP/IP Telnet. Supply an IP address as a standard, four-part dotted decimal IP address, or the name of an IP host that can be resolved by the DNS, or explicit specification in an **ip host** command (refer to the description for the **host-name** keyword in the "Outgoing TCP Connection Request Options" section).

Table 48 X.25-to-TCP Outgoing Options (continued)

Outgoing TCP Connection Request Options

Any of the following optional keywords can be used to configure TCP connection requests:

- **binary**—Negotiates Telnet binary mode on the connection.
- **host-name**—Stores the host name rather than its IP address, thereby allowing the host name to be resolved at connection time instead of configuration time. There is also a **rotor** keyword suboption that you can use to modify the behavior of the **host-name** keyword by allowing one of the IP addresses defined by the **ip host** configuration command to be chosen randomly. If one address fails, another one will be tried, and so on until all address choices are exhausted. You can use the **rotor** keyword, therefore, to provide basic load sharing of the IP destinations.
- **multibyte-IAC**—Always treat multiple Interpret as Command (IAC) escape character codes as a Telnet command.
- **port** *number*—For incoming connections, enter the number of the port to match. The default is port 23 (Telnet).
- **source-interface**—Specifies the source address used for Telnet connections initiated by the router.
- **stream**—Performs stream processing, which enables a raw TCP stream with no Telnet control sequences. A stream connection does not process or generate any Telnet options, and also prevents Telnet processing of the data stream. This option might be useful for connections to ports running UNIX-to-UNIX Copy Program (UUCP) or other non-Telnet protocols, or to ports connected to printers. For ports connected to printers using Telnet, the **stream** keyword prevents some of the problems associated with using Telnet for printers, such as unusual events happening to carriage returns or line feeds and echoing of data back to VMS systems.

Protocol Translation and X.25 PVCs Functional Description

This section describes how the protocol translator works with X.25 PVCs. It will help you understand the overall behavior of incoming and outgoing X.25 PVCs associated with a **translate** command, enabling you to correctly configure protocol translator PVCs for your application.

Configuring X.25 PVCs

When the **translate x25** command is configured with a PVC, an attempt is made to create the PVC. The following conditions can cause this attempt to fail:

- The PVCs assignment of the X.25 interface does not include the PVC number in the **translate x25** command.
- The PVC number in the **translate x25** command is already in use.
- An X.25 destination in a **translate x25** command is routed to X.25 over TCP/IP (XOT), Connection Mode Network Service (CMNS), or Annex G, which do not support translated PVCs.

PVC numbers must be unique across an X.25 connection; however, PVC 1 on Serial 1/0 is different (and therefore unique) from PVC 1 on Serial 2/1.

If, once the **translate x25** command is accepted, the X.25 interface on which the PVC is created goes down, the PVC enters an inactive state, the TCP or LAT connection is terminated, but the existing PAD context remains inactive.

An incoming TCP or LAT connection associated with a down outgoing PVC (displaying a "P/Inactive message") will be rejected by the protocol translator.

2490 Paula
RQS N TR-161 CN
CPMI - CORREIOS
0374
Fls:
3701
Doc:

If any X.25 traffic is received while the corresponding TCP or LAT connection is terminated, and if a Data packet is received in state D1, a Reset with a diagnostic message will be displayed, similar to the following:

```
20:17:11.809: Serial2: X.25 O D1 Reset (5) 8 lci 4
20:17:11.809: Cause 29, Diag 113 (Network out of order (PVC)/Remote network problem)
```

The number of outgoing and incoming protocol translation PVCs is limited only by the number of virtual terminal lines supported on the Cisco router. Remember that each protocol translation session uses a virtual terminal line, which lowers the number of virtual terminal lines available for Telnet sessions.

By default, the Cisco router sends a Reset packet with the cause "PVC Network Operational" and diagnostic "Maintenance action" messages at the start of a TCP or LAT to PVC translation session, to announce that the connection is established and that the PVC is able to handle data traffic. To suppress the PVC Reset packet at TCP or LAT session startup, configure the **no-reset** outgoing PVC keyword as shown in the following example:

```
translate tcp 192.168.22.102 port 5 x25 333 pvc 5 no-reset profile tcl
```

Changing or Removing a translate Command PVC Configuration

Removing a **translate** command with an outgoing PVC specified is allowed only when there no active connection is associated with the outgoing PVC. An attempt to remove an active translation results in the following message:

```
Translate: Can't delete/add entry - Connection(s) are currently active
```

For example, if PVC 5 is assigned to a **translate** command as shown in the following example:

```
translate tcp 10.0.155.61 port 5 x25 5 pvc 5 interface Serial2/0
```

And you want PVC 5 to be assigned under an X.25 interface instead of the **translate** command, as shown in the following example:

```
interface serial2/0
  x25 pvc 5 int s4/0 pvc 25
```

Perform the following steps to configure this reassignment:

Step 1 Check whether a PVC is associated with a serial connection using the **show x25** EXEC command, as follows:

```
Router# show x25 vc 5

PVC 5, State:D1, Interface:Serial2/0
   Started ...

   Line:230 vty 4  Location:Host:nmos3m1
    connected to PAD <--> X25
```

Step 2 If the PVC is associated with a TCP connection, terminate the connection by disconnecting the TCP session or by using the **clear line** EXEC command as shown in the following example:

```
Router# clear line vty 4
```

Step 3 Enter configuration mode, delete the **translate** command, and reassign PVC 5 to an interface:

```
Router(config)# no translate tcp 10.0.155.61 port 5 x25 5 pvc 5 interface Serial2/0
Router(config)# interface serial2/0
Router(config-if)# x25 pvc 5 int s4/0 pvc 25
```

2486
Paula

Related Commands

Command	Description
show translate	Displays configured translation sessions.
translate lat	Translates a LAT connection request automatically to another outgoing protocol connection.
translate tcp	Translates a TCP connection request automatically to another outgoing protocol connection.
x29 access-list	Limits access to the access server from certain X.25 hosts.
x29 profile	Creates a PAD profile script for use by the **translate** command.

ECT N° 03/2005 - CN
CP TR-185 REIOS
0375
Fls:
3701
Doc:

translate x25 (virtual access interfaces)

When receiving an X.25 connection request to a particular destination address, to set up the Cisco router to automatically translate the request to another outgoing protocol connection type, use the **translate x25** command in global configuration mode. To remove or change the translation request, use the **no** form of this command.

The command syntax that follows shows how to apply a virtual interface template in place of outgoing **translate x25** options. If you are using virtual templates for protocol translation, all outgoing options are defined in the virtual interface template. Table 49 lists all outgoing options and their corresponding interface configuration commands.

translate x25 *incoming-address* [*incoming-options* [**pvc** *number* [*pvc-options*]]] *protocol outgoing-address* [*outgoing-options*] **virtual-template** *number* [*global-options*]

no translate x25 *incoming-address* [*incoming-options* [**pvc** *number* [*pvc-options*]]] *protocol outgoing-address* [*outgoing-options*] **virtual-template** *number* [*global-options*]

Syntax Description

incoming-address	An X.25 and X.121 address that conform to specifications provided in the *CCITT 1984 Red Book.* This address generally consists of a portion that is administered by the PDN and a portion that is locally assigned. You must be sure that the numbers that you assign agree with the addresses assigned to you by the X.25 service provider. The X.121 addresses generally will be subaddresses of the X.121 address for the X.25 network interface. Typically, the interface address will be a 12-digit number. Any additional digits are interpreted as a subaddress. The PDN still routes these calls to the interface, and the Cisco IOS software is responsible for interpreting the extra digits. Do not use the same address on the interface and for translation.
incoming-options	(Optional) Incoming connection request keywords and arguments, as follows: • **accept-reverse**—Accepts reverse charged calls on an X.121 address even if the serial interface is not configured to accept reverse charged calls. This is an incoming option only. • **cud** *c-u-data*—Specifies the Call User Data (CUD) field to match in the X.25 Incoming Call packet. If not configured, the CUD in the Incoming Call packet must be blank. • **printer**—Supports LAT and TCP printing over an X.25 network among multiple sites. Provides an "interlock mechanism" between the acceptance of an incoming X.25 connection and the opening of an outgoing LAT or TCP connection. The **printer** keyword causes the protocol translation software to delay the call confirmation of an incoming X.25 call request until the outgoing protocol connection (to TCP or LAT) has been successfully established. An unsuccessful outgoing connection attempt to the router results in the incoming X.25 connection being refused, rather than being confirmed and then cleared, which is the default behavior. Note that using this keyword will force the global **quiet** keyword to be applied to the translation.

2488 Paula

If you want to modify the **translate** command and change the PVC number from 5 to 12, follow steps 1 and 2, and modify the **translate** command with PVC 12, as follows:

```
Router(config)# translate tcp 10.0.155.61 port 12 x25 12 pvc 12 interface Serial2/0
```

Understanding the X.25 Address and the PVC Interface Option on a translate Command

The protocol translator locates the X.121 destination address in the X.25 route table to determine the interface on which to establish the PVC. A more up-to-date, simpler approach uses the **translate** command with the **interface** keyword, which ignores the status of the interface by avoiding referencing the X.25 route table.

For example, instead of configuring an **x25 route** command for each translated PVC, and entering a long X.121 address on the **translate** command, as shown this example:

```
x25 route ^32785223344502 interface Serial1/5
translate tcp 10.0.155.61 port 2502 x25 32785223344502 pvc 1
```

You can simply enter one **translate** command that links the IP port number with the X.121 address and specifies the interface on which to establish the PVC, as follows:

```
translate tcp 10.0.155.61 port 2502 x25 2502 pvc 1 interface Serial 1/5
```

This is the recommended approach and should be adopted in place of **translate** commands that cause the destination address to be looked up in the route table.

Examples

The following example shows how to use the **translate** global configuration command to translate from an X.25 PAD to a LAT device on Network A. It is applied to Router-A. The configuration example includes an access list that limits remote LAT access through Router-A to connections from PAD-C. This example typifies the use of access lists in the Cisco IOS software. The first two lines define the scope of access-list 1. The first line specifies that access list 1 will permit all calls from X.121 address 44444. The caret symbol (^) specifies that the first number 4 is the beginning of the address number.The second line of the definition explicitly denies calls from any other number. (Refer to the appendix "Regular Expressions" in the *Cisco IOS Terminal Services Configuration Guide*, Release 12.2, for details concerning the use of special characters in defining X.121 addresses.)

```
! Define X25 access list to only allow pad-c.
x29 access-list 1 permit ^44444
x29 access-list 1 deny .*
!
! Set up translation.
translate x25 1111101 lat LAT-A access-class 1
```

The following example shows a simple X.25-to-TCP **translate x25** command. Packets coming in X.25 address 652365123 arrive via PVC 1 and are translated to TCP packets and sent out IP address 172.16.1.1.

```
translate x25 652365123 pvc 1 tcp 172.16.1.1
```

The following example shows a more complex configuration that calls an X.29 profile and swaps the default PAD operation of the router to that of an X.25 host. The name of the profile is fullpackets.

```
x29 profile fullpackets 2:0 3:0 4:100 7:21
translate x25 217536124 profile fullpackets tcp Host1 port 4006 swap
```


RGS Nº 0 TR-133 CPMI - CORREIOS 0376 Fls: 3701 Doc:

The following example shows the use of the X.25 incoming protocol **printer** keyword for an incoming X.25 connection:

```
translate x25 55555 printer tcp 172.16.1.1
```

The following examples causes the protocol translator to try connecting to IP address 172.16.1.1 and if that failed, to try IP address 172.16.2.1, and so on through all IP addresses listed in the **ip host** command:

```
ip host my-hosts 172.16.1.1 172.16.2.1 172.16.3.1
translate x25 55555 tcp my-hosts host-name
```

The following example uses the **rotor** keyword to cause the protocol translator to randomly choose one of the IP address listed in the **ip host** command and if it fails to connect, to try another IP address, until all are exhausted:

```
ip host my-hosts 172.16.1.1 172.16.2.1 172.16.3.1
translate x25 55555 tcp my-hosts host1 rotor
```

The following example translates X.25 packets to PPP. It enables routing updates between the two connections:

```
translate x25 12345678 ppp 10.0.0.2 routing
```

The following example permits clients running ARA to connect through the virtual terminal lines of the device to an AppleTalk network:

```
appletalk routing
translate x25 12345678 autocommand arap
  arap enable
  arap dedicated
  arap timelimit 45
  arap warningtime 5
  arap noguest
  arap require-manual-password
  arap net-access-list 614
```

The following example specifies IP pooling from a DHCP server named *D-Server1*. It then specifies that incoming TCP traffic be translated to SLIP. The DHCP server will dynamically assign IP addresses on the outgoing sessions.

```
ip address-pool dhcp-proxy-client
ip dhcp-server D-Server1
translate x25 5467835 ppp ip-pool scope-name D-Server1
```

The following example specifies a local IP pool named Pool2 with IP addresses ranging from 172.18.10.10 to 172.18.10.110. It then specifies that incoming X.25 traffic be translated to PPP. The local IP pool Pool2 will be used to dynamically assign IP addresses on the outgoing sessions.

```
ip-pool Pool2 172.18.10.10 172.18.10.110
translate x25 1234567 ppp ip-pool scope-name Pool2
```

The following example shows how to set the idle timer. X.25 calls are cleared if they are idle for the configured time.

```
translate x25 1234 idle 2 lat Service3
```

2484 Paula

- **profile** *profile*—Sets the X.3 PAD parameters as defined in the profile created by the **x29 profile** command.
- **pvc** *number* [**interface serial** *number* | **packetsize** *in-size out-size* | **windowsize** *in-size out-size*]—Specifies that the outgoing connection is actually a PVC. The *number* argument specifies the virtual circuit channel number of the connection, which must be less than the virtual circuits assigned to the switched virtual circuit (SVC).Only one session is allowed per PVC. Use the following optional keywords and arguments to further define the connection:
  - **interface serial** *number*—Specifies a PVC interface on which to set up the PVC connection.
  - **packetsize** *in-size out-size*—Specifies the input packet size (*in-size*) and output packet size (*out-size*) for the PVC. Valid packet size values are as follows: 16, 32, 64, 128, 256, 512, 1024, 2048, and 4096.
  - **windowsize** *in-size out-size*—Specifies the packet count for input windows (*in-size*) and output windows (*out-size*) for the outgoing translation. Values of *in-size* and *out-size* range from 1 to 127 and must not be greater than the value set for the **x25 modulo** command. You must specify the same value for *in-size* and *out-size*.

virtual-template *number*	Applies the virtual interface template specified by the *number* argument in place of outgoing options.
global-options	(Optional) Translation options that can be used by any connection type and can be one or more of the following: • **access-class** *number*—Allows the incoming call to be used by source hosts that match the access list parameters. The argument *number* is an integer previously assigned to an access list. Standard access list numbers are in the range from1 to 99; expanded standard access lists numbers are in the range 1300 to 1999. • **local**—Allows Telnet protocol negotiations to *not* be translated. • **login**—Requires that the user log in before the outgoing connection is made. This type of login is specified on the virtual terminal lines with the **login** command. • **max-users** *number*—Limits the number of simultaneous users of the translation to *number* (an integer you specify). • **quiet**—Suppresses printing of user-information messages. • **swap**—Valid for X.25-to-TCP translations only, and allows X.3 parameters to be set on the router by the host originating the X.25 call, or by an X.29 profile. This keyword allows incoming and outgoing X.25 connections to be swapped so that the device is treated like a PAD when it accepts a call. By default, the router functions like a PAD for calls that it initiates, and like an X.25 host for calls it accepts. The **swap** keyword allows connections from an X.25 host that wants to connect to the router, and then treats it like a PAD.

RQS Nº 03/2005 - CN
CPMI TR-187 EIOS
0377
Fls:
3701
Doc:

Defaults

No default translation parameters.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

You define the protocol translation connections by choosing a protocol keyword and supplying the appropriate address or service name. The protocol connection information is followed by optional features for that connection, as appropriate. The global options, in general, apply to all the connection types, but there are exceptions. The **swap** keyword, for example, is for X.25- to-TCP translations only. See the example for more explanations on how to enter this command.

Rather than specifying outgoing translation options in the **translate** command, configure these options as interface configuration commands under the virtual interface template, then apply the virtual interface template to the **translate** command. Table 49 maps outgoing **translate** command options to interface commands you can configure in the virtual interface template.

Table 49 Mapping Outgoing translate x25 Options to Interface Commands

translate x25 Command Options	Corresponding Interface Configuration Command
ip-pool	**peer default ip address** {**ip-address** | **dhcp** | **pool** [*poolname*]}
header-compression	**ip tcp header compression** [**on** | **off** | **passive**]
routing	**ip routing** or **ipx routing**
mtu	**mtu**
keepalive	**keepalive**
authentication {**chap** | **pap**}	**ppp authentication** {**chap** | **pap**}
ppp use-tacacs	**ppp use-tacacs**
lpx loópback	**ipx ppp-client loopback** *number*

Examples

The following example shows a virtual template with PPP encapsulation specified by default (not explicit). It also specifies CHAP authentication and an X.29 access list.

```
x29 access-list 1 permit ^5555
!
interface Virtual-Template1
 ip unnumbered Ethernet0
 peer default ip address 172.16.2.129
 ppp authentication chap
!
translate x25 5555667 virtual-template 1 access-class 1
```

Related Commands

Command	Description
interface virtual-template	Creates a virtual template interface that can be configured and applied dynamically in creating virtual access interfaces.
show translate	Displays configured translation sessions.
translate lat	Translates a LAT connection request automatically to another outgoing protocol connection type.
translate tcp	Translates a TCP connection request automatically to another outgoing protocol connection type.
x29 access-list	Limits access to the access server from certain X.25 hosts.
x29 profile	Creates a PAD profile script for use by the **translate** command.

RQS Nº 03/2005 - CN
TR-189
0378
Fls:
Doc 3701

transport input

To define which protocols to use to connect to a specific line of the router, use the **transport input** command in line configuration mode. To change or remove the protocol. use the **no** form of this command.

transport input {all | lat | mop | nasi | none | pad | rlogin | telnet | v120}

no transport input {all | lat | mop | nasi | none | pad | rlogin | telnet | v120}

Syntax Description

all	Selects all protocols.
lat	Selects the Digital LAT protocol and specifies both incoming reverse LAT and host-initiated connections.
mop	Selects Maintenance Operation Protocol (MOP).
nasi	Select NetWare Access Servers Interface (NASI) as the input transport protocol.
none	Prevents any protocol selection on the line. This makes the port unusable by incoming connections.
pad	Selects X.3 packet assembler/disassembler (PAD) incoming connections.
rlogin	Selects the UNIX rlogin protocol.
telnet	Specifies all types of incoming TCP/IP connections.
v120	Selects the V.120 protocol for incoming asynchronous connections over ISDN.

Defaults

No protocols allowed on the line (**none**).

Command Modes

Line configuration

Command History

Release	Modification
10.0	This command was introduced.
11.1	The **none** keyword was added and became the default. Before Cisco IOS Release 11.1, the default keyword was **all**.

Usage Guidelines

Cisco routers do not accept incoming network connections to asynchronous ports (TTY lines) by default. You must specify an incoming transport protocol or specify the **transport input all** command before the line will accept incoming connections. For example, if you are using your router as a terminal server to make console-port connections to routers or other devices, you will not be able to use Telnet to connect to these devices. You will receive the message "Connection Refused." This behavior is new as of Cisco IOS software Release 11.1. Previous to Release 11.1, the default was the **transport input all** command, and the **all** keyword restored pre-Cisco IOS software Release 11.0 defaults. If you are upgrading to Cisco IOS software Release 11.1(1) or later releases from earlier Cisco IOS software Releases, you must configure the **transport input** {*protocol* | **all**} command, or you will be locked out of your router.

2479 Paula

You can specify one protocol, multiple protocols, all protocols, or no protocols. To specify multiple protocols, enter the keyword for each protocol, separated by a space.

This command can be useful in distributing resources among different types of users, or in making certain that only specific hosts can access a particular port. When using two-step protocol translation, the **transport input** command is useful in controlling exactly which protocols can be translated to other protocols.

Access lists for each individual protocol can be defined in addition to the allowances created by the **transport input** command. Any settings made with the **transport input** command override settings made with the **transport preferred** command.

Examples

The following example sets the incoming protocol to Telnet for virtual terminal lines 0 to 32:

```
line vty 0 32
 transport input telnet
```

Related Commands

Command	Description
transport output	Determines the protocols that can be used for outgoing connections from a line.
transport preferred	Specifies the transport protocol that the Cisco IOS software uses if the user does not specify one when initiating a connection.

RQS N TR-191 CN
CPMI - CORREIOS
0379
Fls:
3701
Doc:

transport output

To determine the protocols that can be used for outgoing connections from a line, use the **transport output** command in line configuration mode. To change or remove the protocol, use the **no** form of this command.

transport output {**all** | **lat** | **mop** | **nasi** | **none** | **pad** | **rlogin** | **telnet** | **v120**}

no transport output {**all** | **lat** | **mop** | **nasi** | **none** | **pad** | **rlogin** | **telnet** | **v120**}

Syntax Description

all	Selects all protocols.
lat	Selects the Digital LAT protocol, which is the protocol used most often to connect routers to Digital hosts.
mop	Selects Maintenance Operation Protocol (MOP).
nasi	Selects NetWare Access Server Interface (NASI) as the output transport protocol.
none	Prevents any protocol selection on the line. The system normally assumes that any unrecognized command is a host name. If the protocol is set to **none**, the system no longer makes that assumption. No connection will be attempted if the command is not recognized.
pad	Selects X.3 packet assembler/disassembler (PAD), used most often to connect routers to X.25 hosts.
rlogin	Selects the UNIX rlogin protocol for TCP connections. The rlogin setting is a special case of Telnet. If an rlogin attempt to a particular host has failed, the failure will be tracked, and subsequent connection attempts will use Telnet instead.
telnet	Selects the TCP/IP Telnet protocol. It allows a user at one site to establish a TCP connection to a login server at another site.
v120	Selects the V.120 protocol for outgoing asynchronous connections over ISDN.

Defaults

Telnet

Command Modes

Line configuration

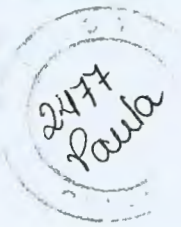
Command History

Release	Modification
10.0	This command was introduced.
11.1	The following keywords were added: • **all** • **lat** • **pad** • **rlogin** • **v120**

Usage Guidelines

You can specify one protocol, multiple protocols, all protocols, or no protocols. To specify multiple protocols, enter the keyword for each protocol, separated by a space.

Any settings made with the **transport output** command override settings made with the **transport preferred** command.



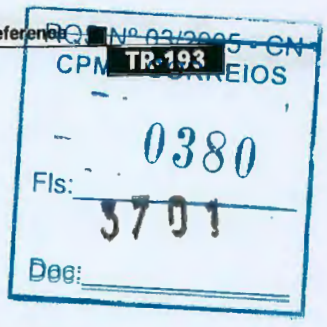
Examples

The following example prevents any protocol selection:

```
transport output none
```

Related Commands

Command	Description
transport input	Defines which protocols to use to connect to a specific line of the router.
transport preferred	Specifies the transport protocol that the Cisco IOS software uses if the user does not specify one when initiating a connection.



transport preferred

To specify the transport protocol that the Cisco IOS software uses if the user does not specify one when initiating a connection, use the **transport preferred** command in line configuration mode. To change or remove the protocol. use the **no** form of this command.

transport preferred {**all** | **lat** | **mop** | **nasi** | **none** | **pad** | **rlogin** | **telnet** | **v120**}

no transport preferred {**all** | **lat** | **mop** | **nasi** | **none** | **pad** | **rlogin** | **telnet** | **v120**}

Syntax Description

all	Selects all recognized protocols.
lat	Selects the Digital LAT protocol, which is the protocol used most often to connect routers to Digital hosts.
mop	Selects Maintenance Operation Protocol (MOP).
nasi	Selects NetWare Access Server Interface (NASI) protocol.
none	Prevents any protocol selection on the line. The system normally assumes that any unrecognized command is a host name. If the protocol is set to **none**, the system no longer makes that assumption. No connection is attempted if the command is not recognized.
pad	Selects X.3 packet assembler/disassembler (PAD), used most often to connect routers to X.25 hosts.
rlogin	Selects the UNIX rlogin protocol for TCP connections. The rlogin setting is a special case of Telnet. If an rlogin attempt to a particular host has failed, the failure will be tracked, and subsequent connection attempts will use Telnet instead.
telnet	Selects the TCP/IP Telnet protocol. It allows a user at one site to establish a TCP connection to a login server at another site.
v120	Selects the asynchronous protocols over ISDN.

Defaults

Telnet

Command Modes

Line configuration

Command History

Release	Modification
10.0	This command was introduced.
11.1	The following keywords were added: • **lat** • **pad** • **rlogin**

Usage Guidelines

Specify the **transport preferred none** command to prevent errant connection attempts.

Any settings made with the **transport input** or **transport output** commands override settings made with the **transport preferred** command.

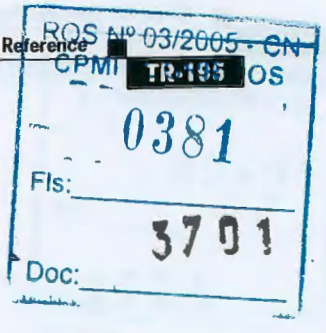
Examples

The following example sets the preferred protocol to Telnet on physical terminal line 1:

```
line tty 1
 transport preferred telnet
```

Related Commands

Command	Description
terminal transport preferred	Specifies the preferred protocol to use for the current session when a command does not specify one.
transport input	Defines which protocols to use to connect to a specific line of the router.
transport output	Determines the protocols that can be used for outgoing connections from a line.



x25 subaddress

To append either a physical port number or a value specified for a line as a subaddress to the X.121 calling address, use the **x25 subaddress** command in line configuration mode. To disable subaddressing, the **no** form of this command.

x25 subaddress {**line** | *number*}

no x25 subaddress {**line** | *number*}

Syntax Description

line	Physical port number for the indicated line to be appended to the X.121 address as the subaddress.
number	Numeric variable assigned to a specific line.

Defaults

No default behavior or values.

Command Modes

Line configuration

Command History

Release	Modification
11.2 F	This command was introduced.

Usage Guidelines

Use the **x25 subaddress line** command to create a unique X.121 calling address by adding either a physical port number or a numeric value for a line as a subaddress to the X.121 calling address.

Examples

The following example shows how to configure subaddressing on virtual terminal lines 10 through 20 by appending the line number as a subaddress to the X.121 calling address:

```
line vty 10 20
x25 subaddress line
```

The following example shows how to configure subaddressing on the first five TTY lines by appending the value 09 as a subaddress to the X.121 calling address of an X.28 connection originating on these lines:

```
line 1 5
x25 subaddress 9
autocommand x28
```

Related Commands

Command	Description
line	Identifies a specific line for configuration and starts the line configuration command collection mode.

A *string sequence* is a two-character capability name followed by an equal sign (=) and the character sequence.

The following example illustrates the capability for homing the cursor:

```
ho=\E[H:
```

The sequence \E represents the ESC character.

Control characters can be represented in *string sequences* by entering a two-character sequence starting with a caret symbol (^), followed by the character to be used as a control character.

The following example illustrates the definition of a control character.

```
bc=^h:
```

In this example, the backspace is entered into the termcap entry as the string sequence as the characters "^h."

A *numeric sequence* is a two-character capability name followed by a number symbol (#) and the number.

The following example represents the number of columns on a screen.

```
co#80:
```

Use the backslash symbol (\ ) to extend the definition to multiple lines. The end of the ttycap termcap entry is specified by a colon terminating a line followed by an end-of-line character and no backslash.

For the definitions of supported Boolean-flag ttycap capabilities, see Table 50. For the definitions of supported string-sequence ttycap capabilities, see Table 51. For the definitions of supported number-sequence ttycap capabilities, see Table 52. For the definitions of supported color-sequence ttycap capabilities, see Table 53.

Table 50 Definitions of ttycap Capabilities: Boolean Flags

Boolean Flag	Description
am	Automatic margin
bs	Terminal can backspace with bs
ms	Safe to move in standout modes
nc	No currently working carriage return
xn	NEWLINE ignored after 80 columns (Concept)
xs	Standout not erased by overwriting (Hewlett-Packard)

Table 51 Definitions of ttycap Capabilities: String Sequences

String Sequence	Description
AL	Add line below with cursor sequence
bc	Backspace if not ^h
bt	Backtab sequence
ce	Clear to end of line
cl	Clear screen, cursor to upper left
cm	Move cursor to row number and column number

2473 Paula
CPMI CORREIOS TR-497 0382 Fls: Doc 3701

Table 51 Definitions of ttycap Capabilities: String Sequences (continued)

String Sequence	Description
cr	Carriage return sequence
cs	Change scrolling region
DL	Delete the line the cursor is on
ei	End insert mode
ho	Home, move cursor to upper left
ic	Character insert
im	Begin insert mode
is	Initialization string (typically tab stop initialization)
ll	Move cursor to lower left corner
md	Turn on bold (extra bright) character attribute
me	Turn off all character attributes
nd	Nondestructive space
nl	Newline sequence
pc	Pad character if not NULL
rc	Restore cursor position
rs	Resets terminal to known starting state
sc	Save cursor position
se	End standout mode (highlight)
so	Start standout mode (highlight)
ta	Tab
te	End programs that use cursor motion
ti	Initialization for programs that use cursor motion
uc	Underline character at cursor
ue	End underline mode
up	Move cursor up
us	Begin underline mode
vb	Visual bell
vs	Visual cursor
ve	Normal cursor

Table 52 Definitions of ttycap Capabilities: Number Sequences

Number Sequence	Description
li	Lines on the screen
co	Columns on the screen
sg	Standout glitch, number of spaces printed when entering or leaving standout display mode
ug	Underline glitch, number of spaces printed when entering or leaving underline mode

Table 53 Definitions of ttycap Capabilities: Color Sequences

Color Sequence	Description
x0	Black
x1	Blue
x2	Red or orange
x3	Pink or purple
x4	Green, which is the default color
x5	Turquoise
x6	Yellow
x7	Gray or white

The ttycap database uses these color sequences to translate IBM directives into screen drawing commands. These color sequences control only foreground terminal colors. They do not control background color, which is configured to black by default.

Examples

The following is an example of a ttycap file. Refer to the chapter "Configuring Dial-In Terminal Services" in the *Cisco IOS Terminal Services Configuration Guide* and the tn3270.examples file in the Cisco ftp@cisco.com directory for more examples.

```
ttycap ttycap1\
d0|vt100|vt100-am|vt100am|dec vt100:do=^J:co#80:li#24:\
cl=50^[[;H^[[2J:bs:am:cm=5^[[%i%d;%dH:nd=2^[[C:up=2^[[A:\
ce=3^[[K:so=2^[[7m:se=2^[[m:us=2^[[4m:ue=2^[[m:md=2^[[1m:\
me=2^[[m:ho=^[[H:xn:sc=^[7:rc=^[8:cs=^[[%i%d;%dr:
```

Related Commands

Command	Description
keymap-type	Specifies the keyboard map for a terminal connected to the line.
terminal-type	Specifies the type of terminal connected to a line.

ECT - CORREIOS
TR-199
0383
Fls:
Rubr:
3701

txspeed

To set the terminal transmit speed (how fast the terminal sends information to the modem), use the txspeed command in line configuration mode. To return to the default setting, use the no form of this command.

txspeed *bps*

no txspeed

Syntax Description

bps	Baud rate, in bits per second (bps).

Defaults

9600 bps

Command Modes

Line configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

Set the speed to match the baud rate of whatever device you have connected to the port. Some baud rates available on devices connected to the port might not be supported on the router. The Cisco IOS software will indicate if the speed you select is not supported.

Examples

The following example sets the transmit speed for line 5 to 2400 bps:

```
line 5
 txspeed 2400
```

Related Commands

Command	Description
rotary-group	Sets the terminal receive speed (how fast the terminal receives information from the modem).
source template	Sets the flow control start character.
terminal txspeed	Sets the terminal transmit speed (how fast the terminal can send information) on the current line and session.

where

To list the open sessions, use the where command in EXEC mode.

where

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced in a release prior to Cisco IOS Release 10.0.

Usage Guidelines

The **where** command displays all open sessions associated with the current terminal line.

The **Ctrl^x, where**, and **resume** commands are available with all supported connection protocols.

Examples

The following is sample output from the **where** command:

```
Router# where

Conn Host              Address          Byte   Idle  Conn Name
   1 MATHOM            192.168.7.21        0      0  MATHOM
*  2 CHAPP             172.18.12.19        0      0  CHAPP
```

The asterisk (*) indicates the current terminal session.

Table 54 describes the significant fields shown in the display.

Table 54 where Field Descriptions

Field	Description
Conn	Name or address of the remote host to which the connection is made.
Host	Remote host to which the router is connected through a Telnet session.
Address	IP address of the remote host.
Byte	Number of unread bytes for the user to see on the connection.
Idle	Interval, in minutes, since data was last sent on the line.
Conn Name	Assigned name of the connection.

Related Commands

Command	Description
show sessions	Displays information about open LAT, Telnet, or rlogin connections.

TR-201
0384
Fls:
Doc:

x25 subaddress

To append either a physical port number or a value specified for a line as a subaddress to the X.121 calling address, use the **x25 subaddress** command in line configuration mode. To disable subaddressing, the **no** form of this command.

x25 subaddress {**line** | *number*}

no x25 subaddress {**line** | *number*}

Syntax Description

line	Physical port number for the indicated line to be appended to the X.121 address as the subaddress.
number	Numeric variable assigned to a specific line.

Defaults

No default behavior or values.

Command Modes

Line configuration

Command History

Release	Modification
11.2 F	This command was introduced.

Usage Guidelines

Use the **x25 subaddress line** command to create a unique X.121 calling address by adding either a physical port number or a numeric value for a line as a subaddress to the X.121 calling address.

Examples

The following example shows how to configure subaddressing on virtual terminal lines 10 through 20 by appending the line number as a subaddress to the X.121 calling address:

```
line vty 10 20
x25 subaddress line
```

The following example shows how to configure subaddressing on the first five TTY lines by appending the value 09 as a subaddress to the X.121 calling address of an X.28 connection originating on these lines:

```
line 1 5
x25 subaddress 9
autocommand x28
```

Related Commands

Command	Description
line	Identifies a specific line for configuration and starts the line configuration command collection mode.

2467 Paula

x28

To enter X.28 mode and access an X.25 network or set X.3 packet assembler/disassembler (PAD) parameters, use the **x28** command in EXEC mode. To exit X.28 mode, use the **no** form of this command.

x28 [**escape** *character-string*] [**noescape**] [**nuicud**] [**profile** *file-name*] [**reverse**] [**verbose**]

no x28 [**escape** *character-string*] [**noescape**] [**nuicud**] [**profile** *file-name*] [**reverse**] [**verbose**]

Syntax Description

escape *character-string*	(Optional) Specifies a character string to use to exit X.28 mode and return to EXEC mode. The character string can be any string of alphanumeric characters. The Ctrl key can be used in conjunction with the character string.
noescape	(Optional) Specifies that no escape character string is defined (user cannot return to EXEC mode). On the console line, the **noescape** option is ignored, and the default escape sequence is used (**exit** command).
nuicud	(Optional) Specifies the network user identification (NUI) data to not be placed in the NUI facility of the call request. Instead the data is placed in the Call User Data (CUD) area of the call request packet.
profile *file-name*	(Optional) Specifies using a user-configured profile of X.3 parameters. A profile is created with the **x29 profile** EXEC command.
reverse	(Optional) Specifies reverse charges for outgoing calls made from the local router to the destination device.
verbose	(Optional) Displays optional service signals such as the called DTE address, facility block, and CUD.

Defaults

Disabled. X.28 mode uses standard X.28 command syntax.

Command Modes

EXEC

Command History

Release	Modification
11.2 F	This command was introduced.

Usage Guidelines

If both the **escape** and **noescape** options are not set, the default escape sequence is used (**exit** command).

X.28 mode is identified with an asterisk (*) router prompt. After you enter this mode, the standard X.28 user interface (with the exception of the escape sequence) is available. From this interface, you can configure a PAD device using X.3 parameters, or you can access an X.25 network.

In X.28 mode, you can set PAD command signals using standard or extended command syntax. For example, you can enter the **clr** command or **clear** command to clear a virtual call. A command specified with standard command syntax is merely an abbreviated version of the extended syntax version.

Table 55 lists the commands available in both standard and extended command syntax.

CPMI - TR-203
0385
Fls:
3791
Doc:

Table 55 Available PAD Command Signals

Standard Syntax	Extended Syntax	Description
break		Simulate an asynchronous break.
call		Place a virtual call to a remote device.
clr	**clear**	Clear a virtual call.
command-signal[1]		Specifies a call request without using a standard X.28 command, which is entered with the following syntax: *facilities-x121-address***D***call-user-data*.
help		Display help information. (See Table 57.)
iclr	**iclear**	Request the remote device to clear the call.
int	**interrupt**	Send an Interrupt Packet.
par? **par**	**parameter** **read**	Display the current values of local parameters. (See Table 56.)
prof	**profile** *file-name*	Load a standard or a named profile.
reset		Reset the call.
rpar?	**rread**	Display the current values of remote parameters.
rset?	**rsetread**	Set and then read the values of remote parameters.
set		Change the values of local parameters. (See Table 56.)
set?	**setread**	Change and then read the values of parameters.
stat	**status**	Request the status of a connection.
selection pad		Set up a virtual call.

1. This is an example of issuing a call request command: the **R,G23,P2-234234Duser1** command.

Table 56 lists the different types of parameters you can set using the **set** *parameter-number*:*new-value* PAD command signal from X.28 mode. Refer to the "X.3 PAD Parameters" appendix in the *Cisco IOS Terminal Services Configuration Guide*, Release 12.2 for more complete information about these parameters. See Table 35 in this publication for a list of ASCII characters.

Table 56 Supported X.3 PAD Parameters

Parameter Number	ITU-T Parameter Name	ITU-T X.3 and Cisco Values
1	PAD recall using a character	Minimum value: 0; maximum value: 126; X.28 PAD user emulation mode default: 1. **Note** Not supported by PAD EXEC user interface.
2	Echo	Minimum value: 0; maximum value: 1; PAD EXEC mode and X.28 PAD user emulation mode defaults: 1.
3	Selection of data forwarding character	Minimum value: 0; maximum value: 255; PAD EXEC mode default: 2 (CR); X.28 PAD user emulation mode default: 126 (~).

Table 56 Supported X.3 PAD Parameters (continued)

Parameter Number	ITU-T Parameter Name	ITU-T X.3 and Cisco Values
4	Selection of idle timer delay	Minimum value: 0; maximum value: 255; PAD EXEC mode default: 1; X.28 PAD user emulation mode default: 0.
5	Ancillary device control	Minimum value: 0; maximum value: 2; PAD EXEC mode default: 0; X.28 PAD user emulation mode default: 1.
6	Control of PAD service signals	Minimum value: 0; maximum value: 255; PAD EXEC mode default: 0; X.28 PAD user emulation mode default: 2. **Note** Not supported by PAD EXEC user interface.
7	Action upon receipt of a BREAK signal	Minimum value: 0; maximum value: 31; PAD EXEC mode default: 4; X.28 PAD user emulation mode default: 2.
8	Discard output	Minimum value: 0; maximum value: 1; PAD EXEC mode and X.28 PAD user emulation mode default: 0.
9	Padding after Return	Minimum value: 0; maximum value: 255; PAD EXEC mode and X.28 PAD user emulation mode default: 0.
10	Line folding	Not supported.
11	DTE speed (binary speed of start-stop mode DTE)	Minimum value: 0; maximum value: 18; PAD EXEC mode and X.28 PAD user emulation mode default: 14.
12	Flow control of the PAD by the start-stop DTE	Minimum value: 0; maximum value: 1; PAD EXEC mode default: 0; X.28 PAD user emulation mode default: 1.
13	Line feed insertion (after a Return)	Minimum value: 0; maximum value: 7; PAD EXEC mode and X.28 PAD user emulation mode default: 0.
14	Line feed padding	Minimum value: 0; maximum value: 255; PAD EXEC mode and X.28 PAD user emulation mode default: 0.
15	Editing	Minimum value: 0; maximum value: 1; PAD EXEC mode and X.28 PAD user emulation mode default: 0.
16	Character delete	Minimum value: 0; maximum value: 127; PAD EXEC mode and X.28 PAD user emulation mode default: 127 (DEL).
17	Line delete	Minimum value: 0; maximum value: 127; PAD EXEC mode default: 21 (Ctrl-U); X.28 PAD user emulation mode default: 24 (Ctrl-X).
18	Line display	Minimum value: 0; maximum value: 127; PAD EXEC mode and X.28 PAD user emulation mode default: 18 (Ctrl-R).
19	Editing PAD service signals	Minimum value: 0; maximum value: 126; PAD EXEC mode default: 0; X.28 PAD user emulation mode default: 2. **Note** Not supported by PAD EXEC user interface.

2465 Paula
RQS TR-205 5 ON
CPMI - CORREIOS
0386
Fls:
3701
Doc:

Table 56 Supported X.3 PAD Parameters (continued)

Parameter Number	ITU-T Parameter Name	ITU-T X.3 and Cisco Values
20	Echo mask	Minimum value: 0; maximum value: 255; PAD EXEC mode and X.28 PAD user emulation mode default: 0. **Note** Not supported by PAD EXEC user interface.
21	Parity treatment	Minimum value: 0; maximum value: 4; PAD EXEC mode and X.28 PAD user emulation mode default: 0. **Note** For additional values that can be selected for parameter 21 and to select parity treatment to conform to the French Transpac public switched data network and its technical specification and utilization of networks standards (STUR), refer to the appendix "X.3 PAD Parameters" in the *Cisco IOS Terminal Services Configuration Guide*, Release 12.2.
22	Page wait	Not supported.

Note Abbreviated X.121 addresses are not supported. Such addresses start with a period, are alphanumeric, and are mapped to a full X.121 address by the PAD.

Table 57 lists the options for the X.28 **help** command.

Table 57 X.28 help Options

Command	Description
help	Describes the **help** PAD command.
help command	Displays the list of available PAD command signals.
help parameter	Displays the list of available X.3 PAD parameters.
help parameter *number*	Displays the specified X.3 PAD parameter and its current value.
help list	Lists the available help subjects.
help profiles	Lists available profiles.
help profile *name*	Displays the specified parameter name and current value.
help *any-PAD-command*	Describes the specified PAD command signal.

You can issue call requests from X.28 mode without using standard X.28 commands by using the following command syntax:

*facilities-x121-address***D***call-user-data*

where:

facilities	Applies X.25 facilities to the outgoing call. The hyphen is mandatory.
x121-address	Specifies the address of the remote X.25 device.
D	Facility request code that specifies CUD for the outgoing call.
call-user-data	Specifies the data that accompanies the call request packet sent to the remote X.25 device.

The following rules apply to all call requests parsed in X.28 mode:

- When an X.121 address specified using standard command syntax is followed by an optional CUD field, the call is placed to the X.121 address.
- When standard command syntax is used, one or more facility request codes can be entered, followed by the code value. Additional facility request codes and values also can be entered. Separate each entry with a comma, followed by a dash. An X.121 address and optional CUD can follow this entry.
- If an X.28 command is not entered, a call request is assumed.
- Ensure that the call request begins with a facility code letter, and that it contains a hyphen (-) followed by a string of digits (the X.121 address). The call request can be terminated by an asterisk (*), a "P," or a "D," followed by some data.
- When using extended command syntax is used, the **call** command uses the facility codes and X.121 address as its operand.
- If facility codes are entered without an X.121 address, remember the codes for the next call. When a call is completed, forget the facility codes until they are once again set.

Table 58 shows examples of parsed call requests.

Table 58 Example X.28 Call Requests

Command	Description
123456789	Calls this X.121 address.
123456789*userdata	Calls this X.121 address, with specified data.
123456789Puserdata	Calls this X.121 address, with specified data.
123456789Duserdata	Calls this X.121 address, with specified data.
Nabcd-123456789	Calls this X.121 address, with NUI set to abcd.
Nabcd,R-123456789	Calls 123456789 with NUI of abcd, and with reverse charging.

Examples

The following example uses the ? command to display the optional X.28 keywords:

```
Router# x28 ?

  debug     Turn on Debug Messages for X28 Mode
  escape    Set the string to escape from X28 PAD mode
  noescape  Never exit x28 mode (use with caution)
  nuicud    All calls with NUI, are normal charge with the NUI placed in Call
            User Data
```


2463 fls
RQS Nº 03/2005 - CN
CPMI - CORREIOS
TR-207
0387
Fls:
3701
Doc:

```
profile    Use a defined X.3 Profile
reverse    All calls default to reverse charge
verbose    Turn on Verbose Messages for X28 Mode
<cr>
```

After you are in X.28 mode, use the **call** PAD signal command to place a virtual call:

```
Router# x28

* call 123456
```

The following example enters X.28 mode with the **x28** EXEC command and configures a PAD with the **set** X.3 parameter command. The **set** command sets the idle time delay to 40 seconds.

```
Router# x28

* set 4:40
```

Related Commands

Command	Description
pad	Logs in to a PAD.

x3

To set X.3 packet assembler/disassembler (PAD) parameters, use the **x3** command in EXEC mode.

x3 *parameter:value*

Syntax Description

parameter:value	Sets the PAD parameters. (See Table 56 in the **x28** command description.)

Defaults

For outgoing connections, the X.3 parameters default to the following:

```
2:1, 3:2, 4:1, 7:4, 16:127, 17:21, 18:19
```

All other parameters default to zero, but can be changed using the **/set** switch keyword with either the **resume** command or the **x3** command.

For incoming PAD connections, the software sends an X.29 SET PARAMETER packet to set only the following parameters:

```
2:0, 4:1, 7:21, 15:0
```

For a complete description of the X.3 PAD parameters, see the appendix titled "X.3 PAD Parameters" in the *Cisco IOS Terminal Services Configuration Guide*.

Command Modes

EXEC

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

You can have several PAD connections open at the same time and switch between them. You can also exit a connection and return to the user EXEC prompt at any point.

To open a new connection, first suspend the current connection by pressing the escape sequence (**Ctrl-Shift-6** then **x [Ctrl^x]** by default) to return to the system command prompt, then open the new connection with the **pad** command.

You can have several concurrent sessions open and switch between them. The number of PAD sessions that can be open is defined by the **session-limit** command.

To switch between sessions you must escape one session and resume a previously opened session. Use the Ctrl^x sequence to escape out of a connection, use the **where** EXEC command to check the connection number, and then use the **resume** command with the connection number to resume the suspended connection. These commands are available with all supported connection protocols.

You can issue any of the following commands to terminate a terminal session:

- **exit**
- **quit**
- **logout**

ROS Nº 03/2005 - CN
CPI TR-209 REIOS
0388
Fls:
Doc: 3701

To display information about packet transmission and X.3 PAD parameter settings, use the **show x25 pad** command.

Examples

The following example shows how to change a local X.3 PAD parameter from a remote X.25 host using X.29 messages, which is a secure way to enable a remote host to gain control of local PAD. The local device is named Router-A. The remote host is named Router-B. The parameters listed in the ParamsIn field are incoming parameters, which are sent by the remote PAD. The parameters listed in the ParamsOut field are parameters sent by the local PAD.

```
Router-A# pad 123456
Trying 123456...Open

Router-B> x3 2:0
Router-B>
Router-A# show x25 pad

tty0, connection 1 to host 123456

Total input: 12, control 3, bytes 35. Queued: 0 of 7 (0 bytes).
Total output: 10, control 3, bytes 64.
Flags: 1,   State: 3,   Last error: 1
 ParamsIn:  1:0, 2:0, 3:0, 4:0, 5:0, 6:0, 7:0,
    8:0, 9:0, 10:0, 11:0, 12:0, 13:0, 14:0, 15:0,
    16:0, 17:0, 18:0, 19:0, 20:0, 21:0, 22:0,
 ParamsOut:  1:1, 2:0, 3:2, 4:1, 5:1, 6:0, 7:21,
    8:0, 9:1, 10:0, 11:14, 12:1, 13:0, 14:0, 15:0,
    16:127, 17:21, 18:18, 19:0, 20:0, 21:0, 22:0,
Router-A#
```

Related Commands

Command	Description
resume (X.3 PAD)	Sets X.3 parameters for PAD connections.

2459 Paula

xremote

To prepare the router for manual startup and initiate an XRemote connection, use the **xremote** command in EXEC mode. This command begins the instructions that prompt you through the connection.

xremote

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

EXEC

Command History

Release	Modification
11.1	This command was introduced.

Usage Guidelines

If you do not use a host computer that supports XDMCP or LAT, you must use manual session startup. Manual session startup involves the following steps:

Step 1 Enable XRemote manually on the router port.

Step 2 Connect to the host computer by using a **telnet**, **lat**, or **rlogin** command, then log in as usual.

Step 3 Set the location of the X display.

Step 4 Start client applications.

Step 5 Return to the EXEC prompt.

Step 6 Enter the **xremote** command to enable XRemote manually again on the server port.

Note In manual operation, the server and X terminal remain in XRemote mode until all clients disconnect or the access server receives a reset request from the X terminal. A session might terminate during startup because you invoked transient X clients that set some parameters (such as **xset** or **xmodmap**) and then disconnected. One session must always be open or the connection resets.

Refer to the *Cisco IOS Terminal Services Configuration Guide* for more information about how to establish XRemote sessions between servers.

ROS Nº 03/2005 - CN
CPMI TR-211 OS
0389
Fls:
Doc: 5791

Examples

The following example starts a manual XRemote session:

```
dialup> xremote
XRemote enabled; your display is dialup:2006
Start your clients and type XRemote again
```

The router replies with a message informing you of your X display location. Use this information to tell the XRemote host the location of your X display server. If no clients are found, you see the following message:

```
No X clients waiting - check that your display is darkstar:2006
```

The following example shows a connection from an X display terminal through a router to a host running client programs:

```
dialup> xremote

XRemote enabled; your display is dialup:2006
Start your clients and type XRemote again

dialup> telnet eureka
Trying EUREKA.NOWHERE.COM (722.18.1.55)... Open

SunOS UNIX (eureka)

login: deal
Password:

Last login: Fri Apr 1 17:17:46 from dialup.nowhere.com
SunOS Release (SERVER+FDDI+DBE.patched) #14: Fri Apr 8 10:37:29 PDT 1994

eureka% setenv DISPLAY dialup:2006
eureka% xterm &
[1] 15439

eureka% logout

[Connection to EUREKA closed by foreign host]

dialup> xremote
Entering XRemote
```

The following procedure shows how an XRemote connection is established for a configuration like the one shown in Figure 2. This example assumes that the administrator has set the display environment variable for the user to identify the X display terminal.

Step 1 From the PCX, MacX, or UNIX machine in Figure 2, the user connects to port 9003 on access server 1. If your administrator has configured a rotary number 7, the user connects to port 10007. For more information about rotary groups, refer to the *Cisco IOS Dial Technologies Configuration Guide*.

Step 2 Access server 1 connects the user to a modem.

Step 3 The modem calls access server 2.

Step 4 The user enters **xremote** at the access server 2 prompt.

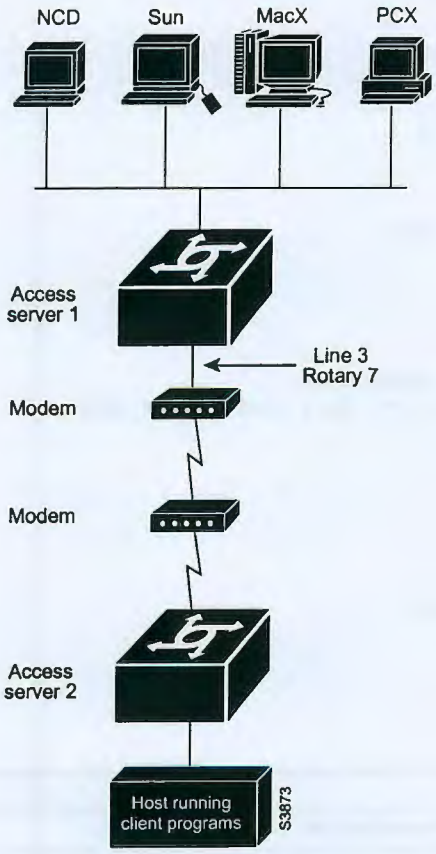
Step 5 The user connects to the host from access server 2 using the **telnet** command.

Step 6 The user starts the X client program that will run on the host and display on the X display server (PCX, MacX, or UNIX host).

Step 7 The user escapes from the host back to the AccessServer2, or logs out if clients were run in the background, and enters the **xremote** command at the AccessServer2 prompt.

You can use the master indexes or search online to find documentation of related commands.

Figure 2 XRemote Session Between Servers



The following example shows how to make an XRemote connection between servers. The number 9016 in the first line of the display indicates a connection to individual line 16. If the administrator had configured a rotary connection, the user would enter 10000 plus the number of the rotary instead of 9016.

```
Router% telnet golden-road 9016

Trying 192.168.7.84 ...
Connected to golden-road.cisco.com.
Escape character is '^]'.

User Access Verification

Password:
Password OK
```


TR-213
CPMI CORREIOS
0390
Fls:
Doc: 3701

```
--- Outbound XRemote service ---
Enter X server name or IP address: innerspace
Enter display number [0]:

 Connecting to tty16... please start up XRemote on the remote system

atdt 13125554141
DIALING
RING
CONNECT 14400

User Access Verification
Username: deal
Password:
  Welcome to the cisco dial-up access server.

dialup> xremote
XRemote enabled; your display is dialup:2006
Start your clients and type XRemote again

dialup> telnet sparks
Trying SPARKS.NOWHERE.COM (172.18.1.55)... Open

SunOS UNIX (sparks)

login: deal
Password:
Last login: Fri Apr 1 17:17:46 from dialup.nowhere.com
SunOS Release (SERVER+FDDI+DBE.patched) #14: Fri Apr 8 10:37:29 PDT 1994

sparks% setenv DISPLAY dialup:2006
sparks% xterm &
[1] 15439

sparks% logout

[Connection to SPARKS closed by foreign host]

dialup> xremote
Entering XRemote
```

Related Commands

Command	Description
xremote lat	Initiates a DECwindow session over a LAT connection.
xremote xdm	Activates automatic session startup for an XRemote connection.

2455 Paula

xremote lat

To initiate a DECwindow session over a local-area transport (LAT) connection, use the **xremote lat** command in EXEC mode.

xremote lat *service*

Syntax Description

service	Name of the desired LAT service.

Command Modes

EXEC

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

If your host computer supports DECwindows login sessions, you can use automatic session startup to make an XRemote session connection. Once the system administrator at the remote host configures support for DECwindows over LAT, use the **xremote lat** EXEC command to initiate the connection. After you issue this command, the following events occur:

- The XRemote font server down-line loads several initial fonts for the DECwindows login display.
- The terminal displays the DIGITAL logo and DECwindows login box.

Log in to the host. Upon completion of login, more fonts are loaded, and the remote session begins.

Note Because of heavy font usage, DECwindows applications can take longer than expected to start when XRemote is used. Once the application starts, performance and access times should be as expected.

To exit XRemote sessions, you must quit all active X connections, usually with a command supported by your X client system. Usually when you quit the last connection (when all client processes are stopped), XRemote closes and you return to the EXEC prompt. However, your X client system determines how the session closes.

Examples

The following example begins connection with a LAT service named service1:

```
xremote lat service1
```

Related Commands

Command	Description
xremote	Prepares the router for manual startup and initiates an XRemote connection.
xremote xdm	Activates automatic session startup for an XRemote connection.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
TR-215
0391
Fls:
3701
Doc:

xremote tftp buffersize

To change the buffer size used for loading font files, use the **xremote tftp buffersize** command in global configuration mode. To restore the buffer size to the default value, use the **no** form of this command.

xremote tftp buffersize *buffersize*

no xremote tftp buffersize

Syntax Description

buffersize	Buffer size in bytes. This is a decimal number in the range from 4096 to 70000 bytes. The default is 70000.

Defaults

70000 bytes

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

When the X terminal requests that a font file be loaded, the Cisco IOS software must first load the font file into an internal buffer before passing it to the X terminal. The default value of 70000 bytes is adequate for most font files, but the size can be increased as necessary for nonstandard font files.

The buffer size can be set as low as 4096 bytes and as large as the available memory on the router will allow. If you are using local-area transport (LAT) font access, you should not lower the buffer size below the default, because the font directory for all of the LAT fonts (created internally) requires 70000 bytes.

This command applies to both TFTP and LAT font access.

Examples

The following example sets the buffer size to 20000 bytes:

```
xremote tftp buffersize 20000
```

2453
Paula

xremote tftp host

To add a specific Trivial File Transfer Protocol (TFTP) font server as a source of fonts for the terminal, use the **xremote tftp host** command in global configuration mode. To remove a font server from the list, use the **no** form of this command.

xremote tftp host *host-name*

no xremote tftp host *host-name*

Syntax Description

host-name	IP address or name of the host containing fonts.

Defaults

No TFTP font server is specified.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

Each time a new host name is entered, the list in the Cisco IOS software is updated. Font servers are queried in the order of their definition when the X terminal requests a font.

Examples

The following example sets the host named IBM-1 as an XRemote TFTP font server:

```
xremote tftp host IBM-1
```

The following example sets the host with IP address 10.0.0.7 as an XRemote TFTP font server:

```
xremote tftp host 10.0.0.7
```


RQS TR-217 - CN
CPMI - CORREIOS
0392
Fls:
Doc: 3701

xremote tftp retries

To specify the number of retries the font loader will attempt before declaring an error condition, use the **xremote tftp retries** command in global configuration mode. To restore the default retries number, use the **no** form of this command.

xremote tftp retries *retries*

no xremote tftp retries

Syntax Description

retries	(Optional) Number of retries. Acceptable values are decimal numbers in the range from 1 to 15.

Defaults

3 retries

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

Under certain conditions, you might need to increase the number of retries, particularly if the font servers are known to be heavily loaded.

Examples

The following example sets the number of font loader retries to 5:

```
xremote tftp retries 5
```

2451 Paula

xremote xdm

To activate automatic session startup for an XRemote connection, use the **xremote xdm** command in EXEC mode.

xremote xdm [*host-name*]

Syntax Description

host-name	(Optional) Host computer name or IP address.

Command Modes

EXEC

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

If your host computer supports a server running X Display Manager Control Protocol (XDMCP) (such as the xdm program included in X11R4 or later), you can use automatic session startup to make an XRemote session connection using the **xremote xdm** EXEC command.

This command sends an XDMCP session startup request to the host computer. If you do not specify a host name or IP address, a broadcast message is sent to all hosts. The first host to respond by starting up a session is used.

The XRemote (the host) server and X terminal stay in XRemote mode until either the display manager terminates the session or the XRemote server receives a reset request from the X terminal.

To exit XRemote sessions, you must quit all active X connections, usually with a command supported by your X client system. Usually when you quit the last connection (all client processes are stopped), XRemote closes and you return to the EXEC prompt. However, your remote X client system determines how the session closes.

To terminate a session, disconnect from the device on the network using the command specific to that device. Then exit from the EXEC by using the **exit** command.

amples

The following example starts a session with a remote host named host1:

```
xremote xdm host1
```

Related Commands

Command	Description
xremote	Prepares the router for manual startup and initiates an XRemote connection.
xremote lat	Initiates a DECwindow session over a LAT connection.

TR-219
CPMI CORREIOS
0393
Fls:
3701
Doc:

Apêndice AQ

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0394
Fls:
3701
Doc:

2450
Paula

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

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0395
Fls:
3701
Doc:

2449
Paula

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

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

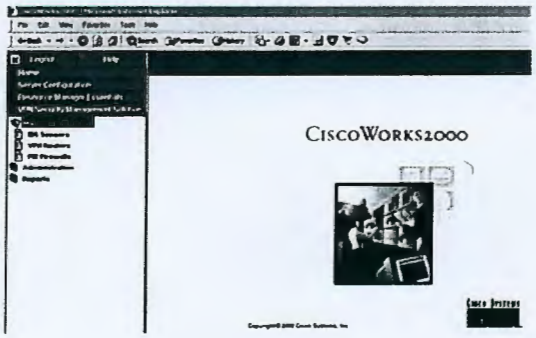
RQS Nº 03/2005 - CN
CPMI - CORREIOS
0396
Fls:
Doc: 3701

2448
Paula

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:

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0397
Fls:
3701
Doc:

2447
Paula

- 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

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 0398
Doc: 3701

- 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

Cisco Systems, Inc.
All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0399
Fls:
Doc:
3701

2445
Fls:

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)

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0400
Fls:
3701
Doc:

- 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.

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0401
Fls:
3701
Doc:

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

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

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Catalyst, Cisco, Cisco Systems, Cisco IOS, the Cisco Systems logo, Cisco Unity, and EtherSwitch are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0303R)

RQS Nº 03/2005 - CN
CMM - CORREIOS
Fls: 402
3701
Doc:

Apêndice AR

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0403
Fls: 3701
Doc:

Cisco VPN 3000 Concentrator Series

2442 Paula

Product Overview

The Cisco VPN 3000 Concentrator Series is a best-of-breed, remote-access VPN solution for enterprise-class deployment. A standards-based, easy-to-use VPN client and scalable VPN tunnel termination devices are included as well as a management system that enables corporations to easily install, configure and monitor their remote access VPNs. Incorporating the most-advanced, high-availability capabilities with a unique purpose-built, remote-access architecture, the Cisco VPN 3000 Concentrator allows corporations to build high-performance, scalable, and robust VPN infrastructures to support their mission-critical, remote-access applications. Unique to the industry, it is the only scalable platform to offer components that are field-swappable and can be upgraded by the customer. These components, called Scalable Encryption Processing (SEP) modules, enable users to easily add capacity and throughput. The Cisco VPN 3000 Concentrator supports the widest range of VPN client software implementations, including the Cisco VPN Client, VPN 3002 Hardware Client, the Microsoft Windows 2000 L2TP/IPsec Client and the Microsoft PPTP for Windows 95, Windows 98, Windows NT, and Windows 2000.

The Cisco VPN 3000 Concentrator is available in five different models to support any business:

Cisco VPN 3005 Concentrator

The 3005 is a VPN platform designed for small- to medium-sized organizations with bandwidth requirements up to full-duplex T1/E1 (4Mbps maximum performance) and up to 100 simultaneous sessions. Encryption processing is performed in software. The 3005 does not have built-in upgrade capability.

Cisco VPN 3015 Concentrator

The 3015 is a VPN platform designed for small- to medium-sized organizations with bandwidth requirements up to full-x T1/E1 (4Mbps maximum performance) and up to 100 simultaneous sessions. Like the 3005, encryption processing is performed in software, but the 3015 is also field-upgradeable to models 3030, 3060, and 3080.

Cisco VPN 3030 Concentrator

The 3030 is a VPN platform designed for medium- to large-sized organizations with bandwidth requirements from full T1/E1 through fractional T3 (50 Mbps maximum performance) and up to 1500 simultaneous sessions. Specialized SEP modules perform hardware-based acceleration. The 3030 is field-upgradeable to the 3060. Redundant and non-redundant configurations are available.

Cisco VPN 3060 Concentrator

The 3060 is a VPN platform designed for large organizations demanding the highest level of performance and reliability, with high-bandwidth requirements from fractional T3 through full T3/E3 or greater (100 Mbps maximum performance) and up to 5000 simultaneous sessions. Specialized SEP modules perform hardware-based acceleration. Redundant and non-redundant configurations are available.

Cisco VPN 3080 Concentrator

The 3080 is 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. The VPN 3080 is available in a fully redundant configuration only.

Cisco VPN Client

Simple to deploy and operate, the Cisco VPN Client is used to establish secure, end-to-end encrypted tunnels to compliant* Cisco Remote Access VPN devices. This thin design, IPSec-compliant implementation is available via CCO download for use with any compliant* Cisco Remote Access VPN product and is included free of charge with the Cisco VPN 3000 Concentrator. The client can be pre-configured for mass deployments and initial logins require very little user intervention.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1
0404
Fls:
3701
Doc:

VPN access policies and configurations are downloaded from the central gateway and pushed to the client when a connection is established, allowing simple deployment and management. The Cisco VPN client provides support for Windows 95, 98, ME, NT 4.0, and 2000.

The Cisco VPN Client is compatible with the following Cisco product versions (compliant Cisco Remote Access products):

- Cisco VPN 3000 Concentrator Release 3.0
- IOS-based platforms (future availability)
- Cisco VPN 5000 Concentrator Release 6.2 and greater (future availability)
- PIX Firewalls Release 6.0 and greater (future availability)

Key Features and Benefits

Cisco VPN 3000 Concentrator Series Features

Table 19-6: Feature Summary for the Cisco VPN 3000 Series

Feature	Cisco 3005	Cisco 3015	Cisco 3030	Cisco 3060	Cisco 3080
Simultaneous Users	100	100	1500	5000	10000
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	N/A	N/A	Option	Option	Yes
Available Expansion Slots	0	4	3	2	N/A
Upgrade Capability	No	Yes	Yes	N/A	N/A
System Memory	32 MB (fixed)	64 MB	128 MB	256 MB	256 MB
T1 WAN Module	Fixed option	Option	Option	Option	Option
Hardware	1U, Fixed	2U, Scalable	2U, Scalable	2U, Scalable	2U
Dual Power Supply	Single	Option	Option	Option	Yes
Client License	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited

The Cisco VPN 3000 Concentrator Series supports the entire range of enterprise applications.

Product Highlights

- High-Performance, Distributed-Processing Architecture
  - —Cisco SEP modules provide hardware-based encryption, ensuring consistent performance throughout the rated capacity (3030 - 3080).
  - —Large-scale tunneling support provided for IPsec, PPTP and L2TP/IPSec connections.
- Scalability (3015-3080)
  - —Modular design (four expansion slots) provides investment protection, redundancy and a simple upgrade path.
  - —System architecture is designed to supply consistent, high-availability performance.
  - —All digital design provides the highest reliability and 24-hour continuous operation.
  - —Robust instrumentation package provides run-time monitoring and alerts.
  - —Microsoft compatibility offers large-scale client deployment and seamless integration with related systems.
- Security

ECT 24411 Paula
ROS Nº 03/2005 - CN
CPMI - CORREIOS
0405
Fls:
Doc: 3701

2440 Paula

—Full support of current and emerging security standards allows for integration of external authentication systems and interoperability with third-party products.

—Firewall capabilities through stateless packet filtering and address translation to assure the required security of a corporate LAN.

—User and group level management offers maximum flexibility.

- High Availability

—Redundant subsystems and multi-chassis fail-over capabilities ensure maximum system uptime.

—Extensive instrumentation and monitoring capabilities provide network managers with real-time system status and early-warning alerts.

- Robust Management

—The Cisco VPN 3000 Concentrators can be managed using any standard Web browser (HTTP or HTTPS), as well as by Telnet, Secure Telnet, SSH, and via a console port.

—Configuration and monitoring capability is provided for both the enterprise and the service provider.

—Access levels are configurable by user and groups, allowing easy configuration and maintenance of security policies.

Specifications

Hardware

Table 19-7: Technical Specifications for Cisco VPN 3000 Series

Description	Specification
Processor	Motorola PowerPC Processor
Ports	Console port-Asynchronous serial (DB-9)
Memory	Redundant system images (Flash) Variable memory options (see chart)
Encryption	3005, 3015: Software encryption 3030, 3060, 3080: Hardware encryption
Embedded LAN Interfaces	3005: Two auto-sensing, full-duplex 10/100BaseTX Fast Ethernet (public/untrusted, private/trusted) 3015- 3080: Three auto-sensing, full-duplex 10/100BaseTX Fast Ethernet (public/untrusted, private/trusted and DMZ)
Instrumentation	3005 Front panel: Unit status indicator 3005 Rear panel: Status light-emitting diodes (LED) for Ethernet ports 3015-3080 Front panel: Status LEDs for system, expansion modules, power supplies, Ethernet modules, fan 3015-3080 Rear panel: Status LEDs for Ethernet modules, expansion modules, power supplies 3015-3080:Activity monitor displays number of sessions, aggregate throughput, or CPU utilization; push-button selectable

Table 19-8: Power Requirements for Cisco VPN 3000 Series

Description	3005	3015 - 3080
Nominal	15 watts (51.22BTU/hr)	35 watts (119.50BTU/hr)
Maximum	25 watts (85.36BTU/hr)	50 watts (170.72BTU/hr)
Input Voltage	100-240VAC	100-240VAC
Frequency	50/60 Hz	50/60 Hz
Power Factor Correction	Universal	Universal

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0406
Fls:
Doc: 3701

12.439
Juno

Table 19-9: Physical and Environmental Characteristics for Cisco VPN 3000 Series

Description	3005	3015	3030	3060	3080
Dimensions (HxWxD)	1.75 x 17.5 x 11.5 in. (4.45 x 44.45 x 29.21 cm)	3.5 x 17.5 x 14.5 in. (8.89 x 44.45 x 36.83 cm)	Same as 3015	Same as 3015	Same as 3015
Weight	8.5 lbs (3.9 kg)	27 lbs (12.3 kg)	28 lbs (12.7 kg)	33 lbs (15 kg)	33 lbs (15 kg)
Operating Temperature	32 to 131°F (0 to 55°C)	Same as 3005	Same as 3005	Same as 3005	Same as 3005
Storage Temperature	-4 to 176°F (-20 to 80°C)	Same as 3005	Same as 3005	Same as 3005	Same as 3005
Humidity	0-to-95% non-condensing	Same as 3005	Same as 3005	Same as 3005	Same as 3005

Table 19-10: Regulatory Approvals for Cisco VPN 3000 Series

Description	Specification
Regulatory Compliance	CE Marking
Safety	UL 1950, CSA
EMC	FCC Part 15 (CFR 47) Class A, EN 55022 Class A, EN 50082-1, AS/NZS 3548 Class A, VCCI Class A

Software

Table 19-11: Software Requirements for Cisco VPN 3000 Series

Description		Specification
Compatibility	Client Software Compatibility	Cisco VPN Client (IPsec) for Windows 95, 98, ME, NT 4.0 and Windows 2000, including centralized split-tunneling control and data compression
		Cisco VPN 3002 Hardware Client
		Microsoft PPTP/MPPE/MPPC
		Microsoft L2TP/IPsec for Windows 2000
		MovianVPN (Certicom) Handheld VPN Client with ECC
	Tunneling Protocols	IPsec, PPTP, L2TP, L2TP/IPsec, NAT Transparent IPsec
	Encryption/ Authentication	IPsec Encapsulating Security Payload (ESP) using DES/3DES (56/168-bit) with MD5 or SHA, MPPE using 40/128-bit RC4
	Key Management	Internet Key Exchange (IKE)
	Routing Protocols	RIP, RIP2, OSPF, Static, Automatic endpoint discovery, Network Address Translation (NAT), Classless Interdomain Routing (CIDR)
	Third-Party Compatibility	Certicom, iPass Ready, Funk Steel Belted RADIUS certified, NTS TunnelBuilder VPN Client (Mac and Windows), Microsoft Internet Explorer, Netscape Communicator, Entrust, GTE Cybertrust, Baltimore, RSA Keon, Verisign
	High Availability	VRRP protocol for multi-chassis redundancy and fail-over
		Destination pooling for client-based fail-over and connection re-establishment
		Redundant SEP modules (optional), power supplies, and fans (3015 - 3060)
		Redundant SEP modules, power supplies, and fans (3080)

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0407
Fls:
Doc 3701

Description		Specification
Management	Configuration	Embedded management interface is accessible via console port, Telnet, SSH, and Secure HTTP
		Administrator access is configurable for five levels of authorization. Authentication can be performed externally via TACACS+
		Role-based management policy separates functions for service provider and end-user management
	Monitoring	Event logging and notification via e-mail (SMTP)
		Automatic FTP backup of event logs
		SNMP MIB-II support
		Configurable SNMP traps
		Syslog output
		System status
		Session data
		General statistics
Security	Authentication and Accounting Servers	Support for redundant external authentication servers:
		- RADIUS (Remote Authentication Dial-In User Service)
		- Microsoft NT Domain authentication
		- RSA Security Dynamics (SecurID Ready)
		Internal Authentication server for up to 100 users
		TACACS+ Administrative user authentication
		X.509v3 Digital Certificates
		RADIUS accounting
	Internet-Based Packet Filtering	Source and destination IP address
		Port and protocol type
		Fragment protection
		FTP session filtering
	Policy Management	By individual user or group
		- Filter profiles
		- Idle and maximum session timeouts
		- Time and day access control
		- Tunneling protocol and security authorization profiles
		-IP Pool
		Authentication Servers

Ordering Information

Product Part Numbers

All part descriptions and part numbers for Cisco products can be accessed using the online Cisco Pricing Tool at

http://www.cisco.com/cgi-bin/order/pricing_root.pl

PROC Nº 53/2005 - CPMI - CORREIOS
Fls: 0408
Doc: 3701

2.438
bmc

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0409
Fls:
3701
Doc:

DOC.
000233

CPL/AC

PREGÃO
050/2003

LOCAÇÃO DE EQUIPAMENTOS DE INFORMÁTICA INCLUINDO ASSISTÊNCIA TÉC NICA E TREINAMENTO

HP INVENT – MANUAL APÊNDICES AS A BU

2003.
PASTA 06

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0410
Fls:
3701
Doc:

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0411
Fls:
3701
Doc:

Cisco Systems

Data Sheet

Cisco **VPN 3000** Series Concentrator

Introduction

The Cisco® VPN Series 3000 Concentrator allow corporations to take full advantage of the unprecedented cost savings, flexibility, performance, and reliability of remote access VPN connections. Corporations use VPNs to establish secure, end-to-end private network connections over a public networking infrastructure. VPNs have become the logical solution for remote-access connectivity for two main reasons:

• Deploying a remote-access VPN enables corporations to reduce communications expenses by using the local dialup infrastructures of Internet service providers.

• Remote Access VPNs allow mobile workers, telecommuters and day extenders to take advantage of broadband connectivity.

To fully realize the benefits of high-performance, remote-access VPNs, a corporation must deploy a robust, highly available VPN solution, and dedicated VPN devices are optimal for this purpose.

The Cisco VPN 3000 Series Concentrator is a best-in-class, remote-access VPN solution for enterprise-class deployment. A standards-based, asy-to-use VPN client and scalable VPN tunnel termination devices are included, as well as a management system that enables corporations to easily install, configure, and monitor their remote access VPNs. Incorporating the most advanced, high-availability capabilities with a unique purpose-built, remote-access architecture, the Cisco VPN 3000 Concentrator allows corporations to build high-performance, scalable, and robust VPN infrastructures to support their mission-critical, remote-access applications.

Unique to the industry, it is the only scalable platform to offer components that are field-swappable and can be upgraded by the customer. These components, called Scalable Encryption Processing (SEP/SEP-E) modules, enable users to easily add capacity and throughput.

The Cisco VPN 3000 Concentrator supports the widest range of VPN client software implementations, including the Cisco VPN Client, the Microsoft Windows 2000/XP L2TP/IPsec Client, the Microsoft L2TP/IPSec VPN Client for Windows 98, Windows Millennium (ME), Windows NT Workstation 4.0, and Microsoft PPTP.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 0412
Doc: 3701

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement

Five Models

The Cisco VPN 3000 Concentrator is available in five different models:

Cisco VPN 3005 Concentrator

The Cisco VPN 3005 Concentrator is a VPN platform 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 sessions. Encryption processing is performed in software. The Cisco VPN 3005 does not have built-in upgrade capability.

Cisco VPN 3015 Concentrator

The Cisco VPN 3015 Concentrator is a VPN platform 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 sessions. Like the Cisco VPN 3005, encryption processing is performed in software, but the Cisco VPN 3015 is also field-upgradable to the Cisco VPN 3030 and 3060 models.

Cisco VPN 3030 Concentrator

The Cisco VPN 3030 Concentrator is a VPN platform designed for medium to large organizations with bandwidth requirements from full T1/E1 through T3/E3(50 Mbps maximum performance) and up to 1500 simultaneous sessions. Specialized SEP modules perform hardware-based acceleration. The Cisco VPN 3030 is field-upgradeable to the Cisco VPN 3060. Redundant and nonredundant configurations are available.

Cisco VPN 3060 Concentrator

The Cisco VPN 3060 is a VPN platform designed for large organizations demanding the highest level of performance and reliability, with high-bandwidth requirements from fractional T3 through full T3/E3 or greater (100 Mbps maximum performance) and up to 5000 simultaneous sessions. Specialized SEP modules perform hardware-based acceleration. Redundant and nonredundant configurations are available.

Cisco VPN 3080 Concentrator

The Cisco VPN 3080 Concentrator is 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. The VPN 3080 is available in a fully redundant configuration only.

ECT 3929 CPI-A

ROS Nº 03/2005 - CN
CPMI - CORREIOS
0413
Fls:
Doc: 3701

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Models Comparison

Table 1 The Cisco VPN 3000 Series Supports the Entire Range of Enterprise Applications

	Cisco VPN 3005	Cisco VPN 3015	Cisco VPN 3030	Cisco VPN 3060	Cisco VPN 3080
Simultaneous Users[1]	100	100	1,500	5,000	10,000
Maximum LAN-to-LAN Sessions	100	100	500	1000	1000
Encryption Throughput	4 Mbps	4 Mbps	50 Mbps	100 Mbps	100 Mbps
Encryption Method	Software	Software	Hardware	Hardware	Hardware
Available Expansion Slots	0	4	3	2	2
Encryption (SEP) Module	0	0	1	2	4
Redundant SEP	–	–	Option	Option	Yes
System Memory	32/64 MB (fixed)	128 MB	128/256 MB	256/512 MB	256/512 MB
Hardware Configuration	1U	Fixed 2U	Scalable 2U	Scalable 2U	Fixed 2U
Dual Power Supply	Single	Option	Option	Option	Yes
Client License	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited

1. For planning purposes, a simultaneous user is considered to be a remote access VPN user connected in all tunneling mode—this includes one IKE Security Association and two unidirectional IPsec SAs (Security Associations). For environments with rekeying or split tunneling, we recommend using a VPN remote access load-balancing environment with spare capacity because these particular sessions will use additional system resources that otherwise would be used to support additional users. The Cisco VPN 3000 Series Concentrator supports the entire range of enterprise applications.

Cisco VPN Client

Simple to deploy and operate, the Cisco VPN Client is used to establish secure, end-to-end encrypted tunnels to the Cisco VPN 3000 Concentrator. This thin design, IPsec-compliant implementation is provided with the Cisco VPN 3000 Concentrator and is licensed for an unlimited number of users. The client can be pre-configured for mass deployments and the initial logons require very little user intervention. VPN access policies are created and stored centrally in the Cisco VPN 3000 Concentrator and pushed to the client when a connection is established.

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0414
Fls:
Doc 3701

Features and Benefits

Product Highlights

High-Performance, Distributed-Processing Architecture

- Cisco SEP modules provide hardware-based encryption, ensuring consistent performance throughout the rated capacity (Cisco VPN 3030–3080).
- Large-scale tunneling support provided for IPsec, PPTP and L2TP/IPsec connections.

Scalability (Cisco VPN 3015–3060)

- Modular design (four expansion slots) provides investment protection, redundancy and a simple upgrade path.
- System architecture is designed to supply consistent, high-availability performance.
- All digital design provides the highest reliability and 24-hour continuous operation.
- Robust instrumentation package provides run-time monitoring and alerts.
- Microsoft compatibility offers large-scale client deployment and smooth integration with related systems.

Security

- Full support of current and emerging security standards allows for integration of external authentication systems and interoperability with third-party products.
- Firewall capabilities through stateless packet filtering and address translation to ensure the required security of a corporate LAN.
- User and group level management offers maximum flexibility.

High Availability

- Redundant subsystems and multichassis failover capabilities ensure maximum system uptime.
- Extensive instrumentation and monitoring capabilities provide network managers with real-time system status and early-warning alerts.

Robust Management

- The Cisco VPN 3000 Concentrator can be managed using any standard Web browser (HTTP or HTTPS), as well as by Telnet, SSHv1, and using a console port. Files can be accessed through HTTPS, FTP, and SSH Copy (SCP).
- Configuration and monitoring capability is provided for both the enterprise and the service provider.
- Access levels are configurable by user and groups, allowing easy configuration and maintenance of security policies. For larger scale deployments, the VPN 3000 Concentrators are supported in several Cisco network management applications. Those applications include:
  - *IP Solution Center (ISC)*—Provisions site-to-site and remote access VPN services
  - *VPN Monitor*—Monitors and reports on remote access and site-to-site VPN tunnel connections
  - *Resource Manager Essentials (RME)*—Provides operational management features such as software distribution, syslog reporting, inventory management
  - *CiscoView*—Provides real time system status monitoring

Cisco Systems, Inc.
All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS Nº 03/2003 - CN
CPMI - CORREIOS
0415
Fls:
Doc: 3701

Technical Specifications

Hardware

Processor

- Motorola PowerPC Processor

Memory

- Redundant system images (Flash)
- Variable memory options (see chart)

Encryption

- *Cisco VPN 3005, 3015*—Software encryption
- *Cisco VPN 3030–3080*—Hardware encryption

Embedded LAN Interfaces

- *Cisco VPN 3005*—Two autosensing, full-duplex 10/100BASE-TX Fast Ethernet (public/untrusted, private/trusted)
- *Cisco VPN 3015–3080*—Three autosensing, full-duplex 10/100BASE-TX Fast Ethernet (public/untrusted, private/trusted and DMZ)

Instrumentation

- *Cisco VPN 3005 Front panel*—Unit status indicator
- *Cisco VPN 3005 Rear panel*—Status LEDs for Ethernet ports
- *Cisco VPN 3015-3080 Front panel*—Status LEDs for system, expansion modules, power supplies, Ethernet modules, fan
- *Cisco VPN 3015–3080 Rear panel*—Status LEDs for Ethernet modules, expansion modules, power supplies
- *Cisco VPN 3015–3080*—Activity monitor displays number of sessions, aggregate throughput, or CPU utilization; push-button selectable

Software

Client Software Compatibility

- Cisco VPN Client (IPsec) for Windows 98, ME, NT 4.0, 2000, XP, Linux (Intel), Solaris (UltraSparc 32 and 64-bit), and Mac OS X 10.2 (Jaguar), including centralized split-tunneling control and data compression
- Microsoft PPTP/MPPE/MPPC, MSCHAPv1/v2, EAP/ RADIUS pass-through for EAP/TLS and EAP/GTC support
- Microsoft L2TP/IPsec forWindows 2000/XP (including XP DHCP option for route population)
- Microsoft L2TP/IPsec for Windows 98, Windows Millennium (ME), and Windows NT Workstation 4.0
- MovianVPN (Certicom) Handheld VPN Client with ECC
- Netlock (Mac OS 8 & 9) VPN Client

Tunneling Protocols

- IPsec, PPTP, L2TP, L2TP/IPsec, NAT Transparent IPsec, Ratified IPsec/UDP (with auto-detection and fragmentation avoidance), IPsec/TCP
- Support for Easy VPN (client and network extension mode)

Cisco Systems, Inc.
All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0416
Fls:
Doc:

Encryption/Authentication

- IPsec Encapsulating Security Payload (ESP) using DES/3DES (56/168-bit) or AES (128, 192, 256-bit) with MD5 or SHA, MPPE using 40/128-bit RC4

Key Management

- Internet Key Exchange (IKE)
- Diffie-Hellman (DH) Groups 1, 2, 5, 7 (ECDH)

Routing

- RIP, RIP2, OSPF, RRI (Reverse Route Injection), static, automatic endpoint discovery, Network Address Translation (NAT), Classless Interdomain Routing (CIDR)
- IPsec fragmentation policiy control, including support for Path MTU Discovery (PMTUD)
- Interface MTU control

Third-Party Compatibility

- Certicom, iPass Ready, Funk Steel Belted RADIUS certified, NTS TunnelBuilder VPN Client (Macintosh and Windows), Microsoft Internet Explorer, Netscape Communicator, Entrust, Baltimore, SA Keon

High Availability

- VRRP protocol for multi-chassis redundancy and fail-over
- Remote Access Load Balancing clusters
- Destination pooling for client-based fail-over and connection re-establishment
- Redundant SEP modules (optional), power supplies, and fans (Cisco VPN 3015–3080)

Management

Configuration

- Embedded management interface is accessible through console port, Telnet, SSHv1, and Secure HTTP (HTTPS)
- Administrator access is configurable for five levels of authorization. Authentication can be performed externally through TACACS+
- Role-based management policy separates functions for service provider and end-user management

Monitoring

- Event logging and notification through e-mail (SMTP)
- Automatic FTP backup of event logs
- SNMP MIB-II support
- Configurable SNMP traps
- Syslog output
- System status
- Session data (including client assign IP, encryption type connection duration, client OS, version, etc)
- General statistics

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 0417
3701
Doc:

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Security

Authentication and Accounting Servers

- Support for redundant external authentication servers:
  - RADIUS
  - Kerberos/Active Directory authentication
  - Microsoft NT Domain authentication
  - Microsoft NT Domain authentication with Password Expiration (MSCHAPv2)

RSA Security Dynamics (SecurID Ready), including native support for RSA 5 (Load Balancing, Resiliency)

- User authorization through LDAP or RADIUS
- Internal Authentication server for up to 100 users
- X.509v3 digital certificates (including CRL/LDAP and CRL/HTTP, CRL Caching and Backup CRL Distribution Point support)
- RADIUS accounting
- TACACS+ Administrative user authentication

Internet-Based Packet Filtering

- Source and destination IP address
- Port and protocol type
- Fragment protection
- FTP session filtering
- Site-to-Site Filters and NAT (for overlapping address space)

Policy Management

- By individual user or group
  - Filter profiles (defined internally or externally)
  - Idle and maximum session timeouts
  - Time and day access control
  - Tunneling protocol and security authorization profiles
  - IP Pool
  - Authentication Servers

Certification

- FIPS 140-2 Level 2 (3.6) in process, FIPS 140-1 Level 2 (3.1), VPNC

Ports

- Console port-Asynchronous serial (DB-9)

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0418
Fls:
3701
Doc:

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Table 2 Physical Characteristics

Concentrator	Cisco VPN 3005	CiscoVPN 3015	Cisco VPN 3030	Cisco VPN 3060	Cisco VPN 3080
Height	1.75" (4.45cm)	3.5" (8.89cm)	3.5" (8.89cm)	3.5" (8.89cm)	3.5" (8.89cm)
Width	17.5" (44.45cm)	17.5" (4.45cm)	17.5" (4.45cm)	17.5" (4.45cm)	17.5" (4.45cm)
Depth	11.5" (29.21cm)	–	–	–	–
Unit without front bezel or SEPS/PS	–	15" (38.1cm)	15" (38.1cm)	15" (38.1cm)	15" (38.1cm)
Unit with front bezel, no SEPS/PS	–	16-3/16" (41.12 cm)	16-3/16" (41.12 cm)	16-3/16" (41.12 cm)	16-3/16" (41.12 cm)
Unit with front bezel and SEPS/PS	–	16.75" (42.55 cm)	16.75" (42.55 cm)	16.75" (42.55 cm)	16.75" (42.55 cm)
Weight	8.5 lbs(3.9kg)	27 lbs(12.3kg)	28 lbs(12.7kg)	33 lbs(15kg)	33 lbs(15kg)

Table 3 Power Type and Requirements

Concentrator	Cisco VPN 3005	CiscoVPN 3015-3080
Nominal	15 watts (51.22BTU/hr)	35 watts (119.50BTU/hr)
Maximum	25 watts (85.36BTU/hr)	50 watts (170.72BTU/hr)
Input Voltage	100-240VAC	100-240VAC
Frequency	50/60 Hz	50/60 Hz
Power Factor Correction	Universal	Universal

Environmental

- Temperature: 32 to 131 F (0 to 55 C) operating; –4 to 176 F (–40 to 70 C) nonoperating
- Humidity: 0 to 95 percent noncondensing

Regulatory Compliance

- CE Marking

Safety

- UL 1950, CSA

EMC

- FCC Part 15 (CFR 47) Class A, EN 55022 Class A, EN50082-1, AS/NZS 3548 Class A, VCCI Class A

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 0419
Doc: 3701

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

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

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Cisco, Cisco Systems, and the Cisco Systems logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0304R)

RD/LW4512 0403

AP AT

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0421
Fls:
3701
Doc:

ECT 397 CPL-AT

Cisco VPN 3000 Series Concentrator

A Remote Access VPN Solution

Introduction

The Cisco VPN 3000 Series Concentrator is a family of purpose-built, remote-access Virtual Private Network (VPN) platforms and client software that incorporates high availability, high performance and scalability with the most advanced encryption and authentication techniques available today.

With the Cisco VPN 3000 Series Concentrator, customers can take advantage of the latest VPN technology to vastly reduce their communications expenditures. Unique to the industry, it is the only scalable platform to offer field-swappable and customer-upgradeable components. These components, called Scalable Encryption Processing (SEP) modules, enable users to easily add capacity and throughput.

Cisco customers can choose from a range of VPN 3000 Concentrator models, the specific unit that most suits their needs and applications. The VPN 3000 Series Concentrator includes models to support a range of enterprise customers, from small businesses with 100 or fewer remote-access users to large organizations with up to 10,000 simultaneous remote users. With all versions of the Cisco VPN 3000 Concentrator, the Cisco VPN Client is provided at no additional charge and includes unlimited distribution licensing.

The Cisco VPN 3000 Series Concentrator is available in both non-redundant and redundant configurations, allowing customers to build the most robust, reliable and cost-effective networks possible. In addition, advanced routing capabilities, such as OSPF, RIP, and Network Address Translation (NAT) are available.

Product Highlights

The Cisco VPN 3000 Series Concentrator upports a wide range of Cisco customer applications in both small- and large-sized enterprise network environments.

High-Performance, Distributed-Processing Architecture

- Cisco SEP modules provide hardware-based encryption, which ensures consistent performance throughout the rated capacity (3030–3080)
- Large-scale tunneling support for IPsec, PPTP and L2TP/IPsec connections

Scalability (3015–3060)

- Modular design (four expansion slots) provides investment protection, redundancy and a simple upgrade path (3015–3060)
- System architecture designed to supply consistent, high-availability performance (3015–3080)
- All digital design, which provides the highest reliability and 24-hour continuous operation (3015–3080)

RQS Nº 03/2005 - CN
CPMI – CORREIOS
0422
Fls: 8
3701
Doc:

Cisco Systems
Copyright © 2001 Cisco Systems, Inc. All Rights Reserved.

- Robust instrumentation package for run-time monitoring and alerts (3015–3080)
- Microsoft® compatibility, which offers large-scale client deployment and seamless integration with related systems (3015–3060)

Security

- Full support of current and emerging security standards, including RADIUS, NT Domain Authentication, RSA SecurID, and digital certificates, allows for integration of external authentication systems and interoperability with third-party products
- Advanced packet-filtering capabilities, which provide the required security for your corporate local-area network (LAN)
- User and group-level management for maximum flexibility

High Availability

- Redundant subsystems and multi-chassis fail-over capabilities for maximum system uptime
- Extensive instrumentation and monitoring capabilities, which provide network managers with real-time system status and early-warning alerts

Robust Management

- The Cisco VPN 3000 Concentrator can be managed using any standard Web browser (HTTP or HTTPS), as well as by Telnet, Secure Telnet, SSH, and via a console port
- Configuration and monitoring capability for both the enterprise and the service provider
- Access levels are configured by user and groups, allowing easy configuration and maintenance of security policies

Cisco VPN Client (IPsec)

- Available for Windows 95, 98, ME, NT 4.0, 2000, XP, Linux (Intel), Solaris (UltraSparc-32bit), and MAC OS X 10.1.
- Centrally configurable policy management, such as split tunneling/local LAN access policy, is pushed down from the Cisco VPN 3000 Concentrator.

Availability and Ordering Information

Pricing and ordering information can be located at http://www.cisco.com/univercd/cc/td/doc/pcat/3000.htm/

A wide variety of service plans are available to support the Cisco VPN 3000 Series Concentrator. Some of these programs include:

Annual Support Plans

Extended Warranty, Enhanced Warranty, 7x24 Installation Support, Remote Telephone Support, Rapid Exchange, Software Subscription

Installation Services

Onsite Installation Service

Time and Materials

Repair and Return, Remote Telephone Support (7x24 or M-F/8 -5), Unit Replacement, Software Update, Hardware Configuration

Cisco Systems
Copyright © 2001 Cisco Systems, Inc. All Rights Reserved.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 0423
Doc: 3701

E C T
399
C P L - E C

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.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 Australia, Pty., Ltd
Level 17, 99 Walker Street
North Sydney
NSW 2059 Australia
www.cisco.com
Tel: +61 2 8448 7100
Fax: +61 2 9957 4350

Cisco Systems has more than 190 offices in the following countries. Addresses, phone numbers, and fax numbers are listed on the

Cisco.com Web site at www.cisco.com/go/offices.

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China • Colombia • Costa Rica • Croatia • Czech Republic • Denmark • Dubai, UAE Finland • France • Germany • Greece • Hong Kong • 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

Copyright © 2001, Cisco Systems, Inc. All rights reserved. PIX and SMARTnet are trademarks, and Cisco, Cisco IOS, Cisco Systems, and the Cisco Systems logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries. All other brands, names, or trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0103R)

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0424
Fls:
3701
Doc:
9401/DA

RQS Nº 03/2005 - C
CPMI - CORREIOS

Fls: 0425

Doc. 3701

Release Notes for Cisco VPN 3000 Series Concentrator, Release 4.0

CCO Date: April 7, 2003

Part Number 78-15416-01

Introduction

Note You can find the most current documentation for released Cisco VPN 3000 products at http://www.cisco.com or http://cco.cisco.com. These electronic documents might contain updates and changes made after the hard-copy documents were printed.

These release notes are for Cisco VPN 3000 Series Concentrator Release 4.0 software. These release notes describe new features, limitations and restrictions, interoperability notes, and related documentation. They also list issues you should be aware of and the procedures you should follow before loading this release. The

CISCO SYSTEMS

Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Copyright © 2003 Cisco Systems, Inc. All rights reserved.

section, "Usage Notes," describes interoperability considerations and other issues you should be aware of when installing and using the VPN 3000 Series Concentrator. Read these release notes carefully prior to installing this release.

Contents

These release notes describe the following topics:

System Requirements, page 2

Upgrading to Release 4.0, page 3

New Features in Release 4.0, page 6

Usage Notes, page 10

Open Caveats for VPN 3000 Series Concentrator, page 16

Caveat Resolved in Release 4.0, page 21

Documentation Updates, page 26

Obtaining Documentation, page 28

Obtaining Technical Assistance, page 30

System Requirements

This section describes the system requirements for Release 4.0.

Hardware Supported

Cisco VPN 3000 Series Concentrator software Release 4.0 supports the following hardware platforms:

- Cisco VPN 3000 Series Concentrators, Models 3005 through 3080
- Altiga Networks VPN Concentrators, Models C10 through C60

Platform Files

Release 4.0 contains two binary files, one for each of two platforms:

- Files beginning with `vpn3000-` support the VPN Concentrator 3015 through 3080 platforms.
- Files beginning with `vpn3005-` support the VPN Concentrator 3005 platform only.

Caution Be sure you install the correct file for the platform you are upgrading.

Upgrading to Release 4.0

This section contains information about upgrading from earlier releases to Release 4.0.

When upgrading VPN 3000 Concentrator releases, you must clear the cache in your browser to ensure that all new screens display correctly when you are managing the VPN Concentrator.

Note You must also log in and click "Save Needed" to add new Release 4.0 parameters to the configuration file. These new Release 4.0 parameters are added to the running configuration immediately, but they are not added to the saved configuration until you click the "Save Needed" or "Save" icon in the VPN Concentrator Manager.

Upgrading to a new version of the VPN 3000 Concentrator software does not automatically overwrite the existing configuration file. Configuration options for new features (for example, IKE proposals) are not automatically saved to the configuration file on an upgrade. The HTML Manager displays "Save Needed" (rather than "Save") to indicate that the configuration needs to be saved. If the configuration is not saved, then on the next reboot, the new configuration options are added again. If you need to send the configuration file to the TAC, save the running configuration to the configuration file first.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
3
Fls: 1
Doc: 3701

Before You Begin

Before you upgrade to this release, *back up your existing configuration to the flash and to an external server.* This ensures that you can return to the previous configuration and software if you need to.

Be aware of the following considerations before you upgrade. These are known product behaviors, and your knowing about them at the beginning of the process should expedite your product upgrade experience. Where appropriate, the number of the caveat documenting the issue appears at the end of the item. See Open Caveats for VPN 3000 Series Concentrator, page 16 for a description of using this number to locate a particular caveat.

Release 4.0 of the VPN 3000 Concentrator software contains several features that interact with corresponding new features in the Release 3.6.x versions of the VPN Client and VPN 3002 Hardware Client software. To get the full benefit of this release you should upgrade your client software as well as your concentrator software. The VPN 3000 Concentrator software, Release 4.0, does operate with VPN Client and VPN 3002 Hardware Client versions 3.0 and higher, but you should upgrade these, too, to take full advantage of the new features.

- To use the VPN Client, Release 3.0 or higher, you *must* upgrade the VPN Concentrator to Release 3.0 or higher. The VPN Client, Release 3.0 or higher, does *not* operate with the VPN 3000 Concentrator version 2.5 or earlier versions.
- Do not update the VPN 3000 Concentrator when the system is under heavy use, as the update might fail (CSCdr61206).
- If you are upgrading from Release 3.0 to Release 3.1 or higher and you are using the "Group Lookup" feature, you must manually set Group Lookup after the upgrade. To enable this feature, go to Configuration | System | General | Authentication and select the Enable check box (CSCdu63961).

Use the following backup procedure to ensure that you have a ready backup configuration.

Backing Up the Existing Configuration to the Flash

1. Go to Administration | File Management | Files.
2. Select the configuration file and click Copy.

3. Enter a name for the backup file (in 8.3 format; for example, name it CON367BK.TST)

You have now backed up the existing configuration to the flash.

Backing Up the Existing Configuration to an External Server

You should also back up the configuration to a server. You can do this in many ways, one of which is to download the file using your Web Browser from the HTML interface (VPN Manager).

You can now upgrade the software with assurance that you can return to your previous firmware using your previous configuration.

Note After upgrading, be sure to clear the cache on your browser. Release 4.0 adds features and enhances HTML page layouts. Clearing your browser cache ensures that everything displays correctly and uses the new features and layout.

Downgrading from Release 4.0

If you need to return to a release prior to Release 4.0, do the following:

Step 1 Reload the firmware for the desired release. (Do not reboot yet.)

Step 2 Rename the existing configuration (for example, rename it as CON367BK.TST).

Step 3 Delete "CONFIG".

Step 4 Copy the previously saved backup file (for example, CON36BKP.TST) to CONFIG. Do not click Save (otherwise, your original CONFIG file will be overwritten with the running configuration).

Step 5 Perform a software reset.

Your prior firmware and image are restored.

New Features in Release 4.0

This section describes the new features in Release 4.0 of the VPN 3000 Series Concentrator. For detailed instructions about how to configure and use these features, see *VPN 3000 Series Concentrator Reference Volume I: Configuration* and *VPN 3000 Series Concentrator Reference Volume II: Administration and Management.*

Hardware Acceleration for Advanced Encryption Standard (AES)

VPN 3000 Concentrator models 3015 and higher now offer an enhanced, scalable encryption processor (SEP-E), that provides hardware support for AES (software support was added in Release 3.6). This feature has no configuration implications. For installation information about the new SEP-E modules, see *Installing SEP or SEP-E Modules in the VPN 3000 Series Concentrator.*

Note The VPN 3000 Concentrator uses *either* SEP or SEP-E modules, not both. Do not install both on the same device. If you install a SEP-E module on a VPN Concentrator that already contains a SEP module, the VPN Concentrator disables the SEP module and uses only the SEP-E module.

512 MB On-Board Memory

You can now upgrade your VPN 3060 or 3080 Concentrator memory to 512 MB.

Note To take advantage of this additional memory, you must also update the VPN Concentrator Manager to Version 4.0 and update the VPN Concentrator Bootcode to Version 4.0.

If your VPN 3000 Concentrator is running low on memory resources, upgrading to 512 MB will help. Symptoms that indicate low memory include the following:

- VPN Concentrator cannot support the necessary number of tunnels.
- VPN Concentrator cannot accept additional connections.
- VPN Concentrator crashes.

To determine the amount of memory currently installed in your VPN Concentrator, use the Monitoring | Status screen. For information about installing memory upgrades and about updating the VPN Concentrator Manager and the VPN Concentrator Bootcode, see *Upgrading Memory to 512 MB in the VPN 3000 Series Concentrator*, included with your memory upgrade kit.

RADIUS User Filters

With Release 4.0, administrators can define remote access user filters in Cisco Secure ACS as download PIX ACLs or as a Cisco vendor-specific RADIUS attribute AV-PAIR (26/9/1), rather than having to define them on each VPN Concentrator. This feature provides limited support for to download inbound access control lists or filters and apply them to a user or group, rather than defining the filters on the VPN Concentrator.

A network administrator can configure the filters on a RADIUS server, rather than on the VPN Concentrator. To provide information about the filter and filter rules, the VPN Concentrator's management system includes a new screen in the monitoring and administration sessions.

Backup LAN-to-LAN

The Backup LAN-to-LAN feature lets you establish redundancy for your LAN-to-LAN connection. Unlike VRRP, which provides a failover for the VPN Concentrator, Backup LAN-to-LAN provides a failover for the connection itself. Although VRRP and Backup LAN-to-LAN are both ways of establishing continuity of service should a VPN Concentrator fail, Backup LAN-to-LAN provides certain advantages that VRRP does not.

- You *can* configure Backup LAN-to-LAN and load balancing on the same device, but you cannot configure VRRP and load balancing on the same VPN Concentrator.
- Redundant Backup LAN-to-LAN peers do not have to be located at the same site. VRRP backup peers cannot be geographically dispersed,

Note This feature does not work in conjunction with VRRP. If you set up a Backup LAN-to-LAN configuration, disable VRRP.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
7
Fls: 0428
Doc: 3701

Native Kerberos Authentication

Release 4.0 supports authentication to Kerberos/Active directory, which is the default authentication mechanism in Windows 2000 and Windows XP. Kerberos is an authentication protocol for use on untrusted networks. The protocol comprises two stages of authentication--the first level is to a key distribution center (KDC), and the second level is between each client and server.

To configure this feature, an administrator must add a Kerberos authentication server on a group basis or add the server to the global authentication servers list and configure such parameters as server IP address, server port, number of retries, and so on. The IPSec group tab includes Kerberos as an authentication type, and statistical displays also include Kerberos authentication statistics.

See the Open Caveats section for information about configuration issues with Active Directory (CSCdz62206) and Linux/UNIX (CSCea20236).

LDAP/RADIUS Authorization

This feature separates user authorization (permissions) from user authentication. It lets certificate users receive permissions by means of LDAP or RADIUS without secondary authentication via XAUTH. It also lets non-certificate users using any type of authentication scheme (Kerberos, NT Domain, SDI, Radius, and Internal) to retrieve these permissions/attributes.

The feature provides a way to configure RADIUS and LDAP authorization servers and event information. The network administrator configures authorization servers on a global system or group basis.

Alerts (Delete with Reason Notifications)

The VPN 3000 Concentrator and the VPN 3002 Hardware Client can send alerts with reasons for disconnects and reboots they initiate to either the VPN Client or Concentrator to which they connect. When a disconnect occurs, the VPN Client displays the disconnect notice and the reason (if available) in the Event log.

The VPN Client can also send alerts regarding disconnects that it initiates, but it does not send a reason.

SNMP Enhancements

With Release 4.0, you can configure a list of particular event identifiers to track, as well as tracking events by class and severity. For more information, see *VPN 3000 Series Concentrator Reference Volume I: Configuration*, Chapter 10, "Events."

Disable LAN-to-LAN Tunnels

With Release 4.0, an administrator can disable a LAN-to-LAN VPN connection without deleting its configuration. This feature can be useful for troubleshooting a connection.

Configurable giaddr for Group-Based DHCP

This feature lets an administrator define a network address on a group basis to be used in DHCP proxy address assignments. To use this feature, DHCP proxy must be enabled on the VPN 3000 Series Concentrator. The administrator enters a network address without a subnet mask under group and user configuration. This address indicates to the DHCP server the scope (that is, the range of available IP addresses on the DHCP server) within which to assign the address.

Memory Conservation Enhancements

Release 4.0 includes modifications to memory structures and allocation algorithms to limit unnecessary memory use.

Memory Statistics Display Enhancements

The VPN 3000 Concentrator and the VPN 3002 Hardware Client now monitor and display memory usage in terms of block size and free and used blocks. The display also includes a new page with detailed statistics.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
9
0429
Fls:
Doc: 3701

Enhanced Sygate Firewall AYT Support

Release 4.0 includes support for Sygate Personal Firewall, Sygate Personal Firewall Pro, and Sygate Security Agent.

Enhanced PING Command Features

- Admin users who have only read access can now do PING commands, using either the Monitor tab on the GUI or the command-line interface. The PING command also appears, as before, on the Admin tab, accessible to users who have full access privileges. The PING command now shows the reply time in milliseconds and not just "device is available."

Adjustable DPD Timeout

For dead-peer detection (DPD), this feature lets an administrator configure the interval that the Concentrator waits before beginning Keepalive monitoring. This feature applies only to Easy VPN Clients that are using IKE Keepalives.

Usage Notes

This section lists interoperability considerations and other issues to consider before installing and using Release 4.0 of the VPN 3000 Series Concentrator software.

Online Documentation

The online documentation might not be accessible when using Internet Explorer with Adobe Acrobat, Version 3.0.1. To resolve this issue, upgrade to Acrobat 4.0 or higher. The latest version of Adobe Acrobat is available at the Adobe web site: http://www.adobe.com.

Disable Group Lock When Using SDI or NT Domain Authentication

This feature is supported only when using Internal or RADIUS authentication. To ensure that you are using this feature properly please refer to the following URL: http://www.cisco.com/warp/customer/471/altigagroup.html

Password Expiry Does Not Change User Profile for LAN

You must enable Start Before Logon on the VPN Client and possibly may need to make sure that DNS and WINS servers are properly configured (CSCdv73252).

Browser Interoperability Issues

The following sections describe known behaviors and issues with the indicated Web browsers.

VPN 3000 Concentrator Fully Supports Only Netscape and Internet Explorer

Currently, the VPN 3000 Concentrator fully supports only Netscape and Internet Explorer. Using other browsers might cause unacceptable behavior; for example, if you attempt to use an unsupported Web Browser to manage the VPN 3000 Concentrator, clicking any of the links might return you to the login screen. (CSCdx87630).

Internet Explorer 4.x Browser Issues

The following are known issues with Internet Explorer 4.X and the VPN Concentrator Manager (the HTML management interface). To avoid these problems, use the latest version of Internet Explorer.

- If you encounter a script error when you try to save your configuration file using Internet Explorer 4.0, reinstall Internet Explorer 4.0, or upgrade to a later version of Internet Explorer. Reinstalling Internet Explorer fixes the problem.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
11
0430
Fls:
Doc: 3701

- If you plan to upgrade the firmware on multiple VPN Concentrators at the same time from the same PC, use the version of Internet Explorer on the Cisco VPN 3000 software distribution media or newer. Using an earlier version could cause a failure in one or more of the upgrades.
- When connecting to the VPN Concentrator using SSL with Internet Explorer 4.0 (v4.72.2106.8), you might receive a message box saying, "This page contains both secure and non-secure items. Do you want to download the non-secure items?" Select Yes. There really are no *non-secure* items on the page and the problem is with Internet Explorer 4.0. If you upgrade to Internet Explorer 4.0 Service Pack 1 or Service Pack 2, you should not see this error message again.

  After adding a new SSL certificate, you might have to restart the browser to use the new certificate.

VPN Client Used with Zone Labs Integrity Agent Uses Port 5054

VPN Clients, when used with the Zone Labs Integrity Agent, are put into a "restricted state" upon connection to the Integrity Server if a port other than 5054 is used. The restricted state simply means the VPN Client is able to communicate only with the Integrity Server; all other traffic is blocked (CSCdw50994).

Workaround:

Do *one* of the following:

- Configure the VPN Concentrator and the Integrity Server to use port 5054 when communicating with each other.
- Edit the WEB.XML file in the Integrity directory and search for 5054 (the port that Integrity uses/looks for). Change it to 5000, save, and restart the Integrity Server.

Administer Sessions Screen Shows Data for Wrong Group

When an L2TP/IPSec connection is established, authentication should behave as follows:

1. The Tunnel Group is authenticated (using the OU field in the Certificate or using the Base Group).

2. The User should be authenticated (using the authentication method of the tunnel group.
3. The User's Group (as defined by the group delimiter option) should be authenticated.

This all works properly, but in the Administration | Administer Sessions screen, the Tunnel Group displays instead of the User's Group (CSCdy00360).

Long Initialization for SNMP Traps in Releases 3.0, 3.5, and 3.5.1

In Releases 3.0, 3.5, and 3.5.1 of the VPN 3000/3002 products, the SNMP task takes 3-5 minutes to complete initialization after a device reboot. Traps being processed during this interval are queued and sent to the SNMP Management station after SNMP task initialization completes.

However, the cold start trap, normally sent as a result of a device rebooting, is never sent.

In Release 2.5.X, the cold start trap is properly sent to the SNMP Manager after a device reboots (CSCdt01583).

Windows NT Authentication Servers Can't Follow Other Server Types in the a Prioritized Authentication Server List

If an Windows NT server follows a non-NT server in the prioritized authentication server list, and the non-NT server becomes unavailable for some reason, the VPN 3000 Concentrator detects this and falls back to the Windows NT server. If the tunnel being established is PPTP or L2TP, the authentication attempt to the Windows NT server also fails.

Therefore, when configuring PPTP or L2TP connections, do not place Windows NT authentication servers behind other types of servers in the applicable authentication server list (CSCdy07226).

RQS Nº 03/2005 - CN - CPMI - CORREIOS
0431
Fls:
3701
Doc:

Accessing Online Glossary Requires Connection to Cisco.com

The Glossary button at the top of all Help screens tries to contact univercd at www.cisco.com (the Cisco documentation site). This connection requires connectivity to Cisco's main web site. If your PC does not have a corporate Internet connection or your firewall blocks access, the following error appears when you attempt to access the Glossary:

"The page cannot be displayed."

To access the Glossary, you must be connected to www.cisco.com (CSCdy14238).

SNMP Traps VRRP Notifications and cipSecMIBNotifications Are Not Supported

The VPN 3000 Concentrator does not support the VRRPNotifications and cipSecMIBNotifications SNMP traps. You can configure VRRP for these SNMP traps without getting an error message, but the traps themselves are not supported, so no action occurs. The same is true of Cisco IPSec-flow MIB notifications (CSCdx44580).

RSA Allows a CA to Issue Only One Certificate with any DN

The rekey option to renew an SSL certificate from the RSA CA results in a rejection of the request.

The resubmit/renew feature does work with RSA as long as the certificate being rekeyed or renewed is first deleted from the CA database. RSA does not allow a CA to issue more than 1 certificate with any particular DN (CSCdv27743).

Reauthentication on Rekey Interval

If you have enabled the Reauthentication on Rekey feature, the VPN Concentrator prompts users to enter an ID and password during Phase 1 IKE negotiations and also prompts for user authentication whenever a rekey occurs. Reauthentication provides additional security.

If the configured rekey interval is very short, users might find repeated authorization requests inconvenient. In this case, disable reauthentication. To check your VPN Concentrator's configured rekey interval, see the Lifetime Measurement, Data Lifetime, and Time Lifetime fields on the Configuration | System | Tunneling Protocols | IPSec | IKE Proposals | Add or Modify screen.

Note At 85% of the rekey interval, the software client prompts the user to reauthenticate. If the user does not respond within approximately 90 seconds, the VPN Concentrator drops the connection.

VPN 3000 Concentrator Ignores RADIUS Packets Longer Than 4096 Bytes

Some RADIUS Servers exceed the Maximum RADIUS packet size of 4096 bytes. The VPN 3000 Series Concentrator ignores RADIUS packets that exceed this length (CSCdz90027).

Downgrading to Release 3.6 with a Release 4.0 Configuration Deletes Information from LAN-to-LAN Groups

A VPN Concentrator with more than 125 users and groups combined fails to terminate tunnels if the SEPs are not active. This is because a VPN Concentrator with no active SEPs is considered to be a model 3015, and model 3015 supports only 125 users and groups combined.

This condition could unexpectedly arise if a VPN Concentrator with a SEP-E, running Release 4.0, is downgraded to Release 3.6. This would result in the problem, because the Release 3.6 does not support the SEP-E module. The SEP-Es are detected as unknown cards if present when running Release 3.6 code.

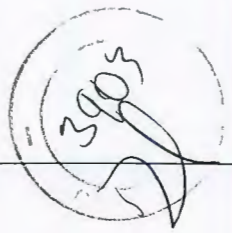
If you encounter a situation, for whatever reason, where you are trying to load a configuration with more users than are supported by the model, the following event appears on the console after a reboot:

****

3 03/20/2003 14:03:16.260 SEV=3 CONFIG/32 RPT=1

ECT 3401 CPLAN

ROS Nº 03/2005 CN
CPI 15 REIOS
Fls: 0432
3701
Doc:



SERVE Too Many Entries Error. Delete an entry before adding a new one.

****

(CSCea51435)

VPN Client Supports Elevated Privileges Using the MSI Installer

Windows Installer 2.0 must be installed on a Windows NT or Windows 2000 PC prior to configuring the PC for a Restricted User with Elevated Privileges When using elevated privileges, the VPN Client program files are created under the specific user, not "ALL" users. (CSCea37900).

Open Caveats for VPN 3000 Series Concentrator

Caveats describe unexpected behavior or defects in Cisco software releases. The following list is sorted by identifier number.

Note If you have an account with CCO, you can use Bug Navigator II to find caveats of any severity for any release. To reach Bug Navigator II on CCO, select Software & Support: Online Technical Support: Software Bug Toolkit or navigate to http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl.

The following problems exist with the VPN 3000 Series Concentrator, Release 4.0.

- CSCds44095

  L2TP over IPSec connections fail if going through a NAT device. During the connection establishment, the VPN Client and the VPN 3000 Concentrator exchange IP addresses. When the client sends what it believes to be the VPN 3000 Concentrator's address (really the NATed address), the VPN 3000 Concentrator releases the connection.

  This is because the address assigned to the interface does not match the address coming in from the client. The same issue exists on the client side. This will not be resolved until the Windows 2000 MS client supports UDP encapsulation.

- CSCdt08303

  When configuring a LAN-to-LAN connection with IOS or PIX, it is important to match the keepalive configuration (both "ON" or both "OFF"). If the keepalive configuration is OFF for the VPN 3000 Concentrator and ON for the IOS device, the tunnel will be established with data.

  IOS tears down the tunnel because the VPN 3000 Concentrator does not respond to IOS style keepalives if keepalives are configured to be OFF for the VPN 3000 Concentrator.

- CSCdw36613

  In some cases, the Zone Labs Integrity Agent may not properly update on the Windows NT version 4.0 operating system while the VPN Client is connected, policy is changed and re-deployed, and the connection is up. Specifically, if you "Block Internet Servers" under the Firewall Security Rules in the Policy and then Deploy that new policy, a PC running Windows NT version 4.0 receives the updated policy, but it might not put the "Block Internet Servers" setting of that policy into effect.

  Workaround:

  Reboot the operating system.

- CSCdx47596

  Due to a Microsoft bug, Windows XP PCs are not capable of receiving a large number of Classless Static Routes (CSR). The VPN 3000 Concentrator limits the number of CSRs that are inserted into a DHCP INFORM message response when configured to do so.

  The VPN 3000 Concentrator limits the number of routes to 28-42, depending on the class.

- CSCdx89348

  The Concentrator may display the following events during a VPN Client connection. These events were found to be due to the client being behind a Linksys Cable/DSL router that was incorrectly modifying the Client's packets, causing them to fail authentication when received by the VPN Concentrator. The problem is more prominent if LZS compression is used.

  Events:

  131500 06/20/2002 17:08:34.300 SEV=4 IPSEC/4 RPT=4632

  IPSec ESP Tunnel Inb: Packet authentication failed, username: gray, SPI:

RQS Nº 03/2005 - CN - CPMI - CORREIOS
17
0433
Fls:
Doc: 3701

4e01db67, Seq Num: 0000850f. Dump of failed hash follows.

Linksys has been notified about the problem.

Workaround:

Although no workaround currently exists, disabling LZS compression on the Concentrator helps reduce the number of events. To disable LZS compression on the Concentrator set the "IPComp" setting on the IPSec tab of the group configuration to "none".

- CSCdy26161

  The Microsoft L2TP/IPSec client for Windows 98, Windows ME, and Windows NT does not connect to the VPN 3000 Concentrator using digital certificates.

  Workaround:

  Use Preshared keys.

- CSCdy27564

  The Assigned IP address for a PIX-501 in Network Extension Mode appears on the VPN 3000 Concentrator as 0.0.0.0 until the first IPSec/Phase 2 rekey takes place. After the Phase 2 rekey completes, the Assigned IP address is correctly set to the PIX-501's private interface network address.

- CSCdz24882

  Using Microsoft Internet Explorer version 5.0, you cannot create a detailed memory report from the Monitoring | System Status | Memory Status | Detailed Memory Report button. The file memory.txt is *not* created. The report does work if the file already exists. You *can* create the file initially if you run a detailed report from the CLI interface. Internet Explorer version 5.5 and Netscape work fine.

- CSCdz83332

  When switching between tabs under the interfaces section of the html-management page, the action may eventually fail.

  If this happens simply go back to the interface summary page and drill back down into the desired interface. Everything will resume working again.

- CSCdz87108

  The LDAP Authorization failure reasons depend on how the LDAP server implements these error codes. RFC 1777-LDAP states that the LDAP server might not return an error code, therefore in those situations the VPN 3000 failure reason is "Invalid response received from server".

  For the case in which the LDAP server *does* return a specific error diagnostic (for example, noSuchAttribute) the VPN 3000 failure reason displays the appropriate string.

- CSCea20236

  Before you use the VPN Concentrator to authenticate a user to a Linux or Unix server running a Kerberos server, follow these steps:

  a. Check the keys available for the user you want to authenticate. Run:

     kadmin.local -q "getprinc *username*"

  b. Make sure that "DES cbc mode with RSA-MD5, Version 5" is one of the available keys. If you do not see "DES cbc mode with RSA-MD5, Version 5", edit the kdc.conf file and add or move des-cbc-md5 selections to the beginning of the supported_enctypes = line. For example:

     [realms]

     MYCOMPANY.COM = {

     master_key_type = des-cbc-crc

     supported_enctypes = des-cbc-md5:normal des-cbc-md5:norealm des-cbc-md5:onlyrealm

     Save the file. Then, restart the krb5kdc, kadmin, and krb524 services.

  c. To create the "DES cbc mode with RSA-MD5" keys, change the users password:

     kadmin.local -q "cpw -pw newpassword *username*"

  Now you should be able to authenticate that user to your Linux/Unix Kerberos 5 server.

- CSCea29828

  HTTP Software Updates sometimes fail with "Software Update Error". Retrying the operation does not update the image.

  Workarounds:

POC Nº 03/2005 - CN
CPMI - [redacted] S
Fls: 0434
Doc: 3701

Do *one* of the following:

- Perform the Software Update using the CLI/telnet interface.
- Reboot the VPN 3000. Performing an HTTP Software Update will now succeed.

- CSCea46018

  When a backup SEP-E fails over to Software, the Activity LED and Status LED stay green, even though the SEP-E is no longer operational.

- CSCea52820

  The text from the Help page for the Monitoring | System Status | Memory Details page in HTML incorrectly refers to "Memory Detail Report". The page is labelled and called: "Detailed Memory Report".

- CSCea52936

  The Help for the SEP-E in the Monitoring | System Status | SEP in-line SEP page is incomplete. In other sections, we make reference to the SEP-E. We should add:

  "AES (SEP-E only)" to the Encryption and Decryption bullet.

  This screen displays status and statistics for a VPN Concentrator SEP (Scalable Encryption Processing) or a SEP-E (Enhanced SEP) module, which performs hardware-based cryptographic functions:

  - Random-number generation.
  - Hash transforms (MD5 and SHA-1) for authentication.
  - Encryption and decryption (DES and Triple-DES).

  The screen shows cumulative data since the system was last booted or reset.

- CSCea69156

  LDAP Authorization to a Microsoft Active Directory LDAP server using authenticated Bind requests is not supported in this release. Only anonymous Binds are currently supported.

Caveat Resolved in Release 4.0

Release 4.0 resolves the following issues:

- CSCdy09630

  The description of the IPSec Backup Servers feature in the VPN 3000 Concentrator Series Reference documentation indicates that it applies only to the VPN3002 Hardware Client. The feature now applies to the Software Client as well. For information about this feature and how to configure it, on the VPN Concentrator, see *VPN Client Administrator Guide*, Chapter 1. For information about how to configure Backup Servers in the VPN Client, see *VPN Client User Guide*.

- CSCdy12056

  If a LAN-to-LAN tunnel between a VPN 3000 Concentrator and an IOS device is misconfigured and repeatedly fails to establish, then the VPN 3000 Concentrator could enter a state where a reboot is required.

  One way to encounter this problem is to try to setup IOS to handle both LAN-to-LAN tunnels and Remote Access tunnels on the same interface, without breaking the IOS interface into V-LANs. This is a misconfiguration and is not supported by IOS, but it can lead to problems with the VPN 3000 Concentrator.

  This configuration is not supported because IOS does not allow the same crypto map to be used to terminate both LAN-to-LAN tunnels and Remote Access tunnels. In addition, IOS only allows one crypto map to be applied per interface.

  Consequently, if both types of tunnels must be terminated on a single physical interface, that interface must be broken out into V-LANs. Dividing the physical interface in this way enables a different crypto map to be applied to each virtual interface. This in turn enables both types of tunnels to be terminated on the same physical interface while maintaining a valid configuration.

- CSCdy26296

  When viewing bandwidth management statistics via the CLI, with Bandwidth Management enabled and multiple users connected, all user sessions scroll through on the screen without the user being prompted to press space to continue or Q to quit.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
21
Fls: 3701
Doc:

- CSCdy28464

  Documentation for the Bandwidth Management feature in Release 3.6.1 refers to a configuration option in which bandwidth aggregation is automatically applied to a LAN-to-LAN connection when a bandwidth reservation policy is applied to a LAN-to-LAN connection. This feature is not available in Release 3.6.1.

  To ensure that bandwidth is always available for a LAN-to-LAN connection via the HTML interface, navigate to Configuration | User Management | Groups. Highlight the LAN-to-LAN group, and select the Assign Bandwidth Policies button. Select the public interface, and next to the Bandwidth Aggregation parameter, enter the amount of bandwidth to reserve from the total available bandwidth for this connection.

  If bandwidth aggregation is not set for a LAN-to-LAN connection, a situation might occur where there is not enough bandwidth available for the tunnel to be established.

- CSCdz48220

  The VPN 3000 Concentrator continually requests the node secret from the RSA server. The RSA server considers these requests as failed login attempts by the RSA server; therefore, the user's account is disabled.

  This problem occurs under the following conditions:

  - The VPN 3000 Concentrator does not have the node secret stored locally.
  - The VPN Client provides an incorrect passcode.

- CSCdz48332

  If you add and delete filters through the GUI interface (Configuration |System |Policy Management | Traffic Management | Filters), there is a very small memory leak for each filter created and deleted.

- CSCdz48402

  The VPN 3000 Concentrator does not consistently send Delete with Reason messages to all the connected clients when you do Reboot *NOW*. The VPN Clients believe they are still connected, but they will eventually disconnect due to the Client's Dead-Peer-Detection mechanism.

- CSCdz53656

  Authorization server statistics are not available in this release.

- CSCdz62206

  If you use Active Directory/Kerberos authentication on the VPN 3000 Concentrator and would like to authenticate to a Windows 2000 or .NET Active Directory server, you *must* change *all* the users' Account options to "Use DES encryption types for this account". This is *required* because the Release 4.0 VPN 3000 Concentrator uses DES encryption, but Windows Active Directory uses RC4.

- CSCdz71450

  When using Active Directory/Kerberos for authentication, if the user types in the username or password incorrectly, the VPN 3000 Concentrator simply ends the connection after the first failure. The user should be prompted three times before failing as it does when using Internal, Radius, or NT Domain authentication methods.

- CSCdz77794

  On the Monitoring | Statistics | Authentication and Monitoring | Statistics | Accounting screens, if you click Reset, then all group-based statistics show up with the Group column=Base Group. In order to show group-based statistics again, click Restore.

- CSCdz78109

  SEP-E to SEP-E failover and SEP-E to software failover are *not* supported in Beta releases.

  New connections are not accepted after SEP-E failover with several calls previously connected and passing data.

- CSCdz79541

  Duplicate of CSCdz85139.

- CSCdz83301

  If a simple password is configured under the OSPF tab, in any of the interface configuration pages, the deleted entry will re-appear even after deleting the password, selecting none for OSPF authentication and clicking apply.

- CSCdz84481

  When a user fails authentication due to a restriction placed on the account at the Active Directory server, the VPN 3000 Concentrator Events do not display the reason for the failure. Some restrictions on the account could be

Account Expired, Account Disabled, Account Locked-Out, Not within Logon Hours and Password Change required. For most of these restrictions you will see the following Events:

124 01/20/2003 11:12:55.590 SEV=10 AUTHDECODE/43 RPT=4

Kerberos: Error type: Client's creds have been revoked

130 01/20/2003 11:12:55.590 SEV=4 AUTH/9 RPT=9 70.139.1.5

Authentication failed: Reason = Invalid response received from server handle = 196, server = 198.133.219.25, user = myuser

- CSCdz85139

  When you add an LDAP Authorization server, the events refer to the server with "type=TACACS+."

- CSCdz87048

  The VPN 3000 Concentrator may leak memory when a VPN Client connects and downloads and ACL User Filter from the RADIUS Server. The amount of memory leaked is closely associated with the size of the actual filter.

- CSCdz87381

  If you externally authenticate Groups and Users to a RADIUS Server, the User filters assigned by the RADIUS Server get corrupted. It is recommended that you authenticate the Groups locally on the Concentrator and the Users externally on a RADIUS Server when utilizing the RADIUS User Filter feature.

- CSCea02122

  RADIUS based user filters are not cleared from the Concentrator when PPTP or L2TP connections are terminated.

- CSCea03407

  Using Netscape version 4.7, under Admin | Admin Sessions, the RADIUS User ACL filters get displayed in a narrow 1 inch wide column with no scroll capabilities. The filters are displayed correctly under Monitoring | Dynamic filters.

- CSCea12148

  If your VPN Concentrator has a SEP-E installed, you might see the following event message when you boot:

CAPI-RSA PKCS1 payload to be decrypted is not in PKCS1 format, bad block type=[0x7][0xb8].

If you receive this event, you will be unable to use HTTPS to manage the VPN Concentrator. To workaround this problem, delete the SSL certificate (from the Administration | Certificate Management screen), then generate a new SSL certificate.

- CSCea13002

  The functionality that allows the administrator to create a network list, from within a LAN-to-LAN configuration page, has changed.

  In previous releases, the user could create a network list from within the LAN-to-LAN configuration page. The new method for creating a network list uses a link on the LAN-to-LAN index page to the network list configuration page.

  This change was resolves a problem with Reverse Route Injection when the network lists are added from within the LAN-to-LAN page. With the previous method, the routes, corresponding to the network lists that were added via the LAN-to-LAN page, were not present in the routing table.

- CSCea16255

  When Strip Realm is disabled, accounting requests should be sent as user name=user. But instead, accounting requests are incorrectly sent with user name=user@realm (Duplicate of CSCea44988).

- CSCea20412

  Using Authentication=RADIUS with Expiry, the VPN Concentrator establishes the tunnel but skips either RADIUS or LDAP authorization.

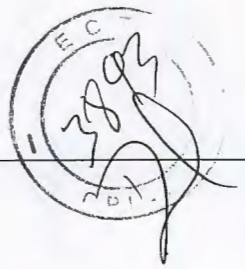
- CSCea24328

  When using Kerberos/Active Directory authentication, if a user types a username with the "@" symbol and Realm using all lowercase for the realm (that is, usernam@mycompany.com instead of username@MYCOMPANY.COM), the following error occurs on the VPN Concentrator, and the Kerberos server status changes to "Not-in-service".

  78 02/19/2003 16:59:49.250 SEV=7 AUTHDBG/76 RPT=8
  Unable to correlate received message with authentication session

  83 02/19/2003 16:59:53.150 SEV=4 AUTH/15 RPT=76
  Server name = 100.136.50.2, type = KERBEROS,
  group = KerberosGroup, status = Not-in-service

RQS Nº 03/2005 - CN
CPMI - CORREIOS
25
0436
Fls:
3701
Doc:



When using Kerberos/Active directory for authenticating, users should enter only their username, username@REALM.COM with Realm all in UPPERCASE letters, or use the Strip Realm setting for the Group on the Concentrator.

- CSCea25668

  Statically assigned filters take precedence over dynamically assigned filters. It should be the other way around.

Documentation Updates

The Cisco VPN 3000 Series Concentrator documentation set has been revised for this release and is available online through Cisco Connection Online (CCO). This section contains any changes and corrections to the documentation that occurred after the documentation was published.

Documentation Changes

The following document requires modifications, reflecting product changes, as noted in the following sections:

- *VPN 3000 Series Concentrator Reference Volume I: Configuration*

Changes to *VPN 3000 Series Concentrator Reference Volume I: Configuration*

Please note the following changes to the Configuration manual.

Syslog Servers Now Supported on Both Windows and UNIX Operating Systems

The VPN 3000 Concentrator now supports syslog servers on both Windows and UNIX (Linux and Solaris) operating system platforms. In *VPN 3000 Series Concentrator Reference Volume I: Configuration,* Chapter 10, "Events," and in the corresponding online Help, the text and the screen captures refer to UNIX syslog servers. This restriction on the type of syslog server operating environment no longer exists.

Inbound Firewall Rules Must Not Limit Traffic to UDP Source Port 4500

In *VPN 3000 Series Concentrator Reference Volume I: Configuration,* Chapter 7, "Tunneling Protocols," make the following change to the note on page 7-35, under Tunneling Protocols | Configuration | System | Tunneling Protocol | IPsec | NAT Transparency area, regarding IPsec over NAT-T:

Note The source port of the client may vary from UDP 4500 especially when traversing a PAT device, so any inbound firewall rules must not specifically limit traffic to a source port of 4500.

VPN 3000 Concentrator Documentation Updates

In addition to these Release Notes, the following documents are new or have been updated for Release 4.0:

- *VPN 3000 Series Concentrator Reference Volume I: Configuration*
- *VPN 3000 Series Concentrator Reference Volume II: Administration and Management*
- *VPN 3000 Series Concentrator Getting Started*
- Online Help

Related Documentation

- *VPN Client User Guide for Windows*
- *VPN Client Administrator Guide*
- *VPN 3002 Hardware Client Getting Started*
- *VPN 3002 Hardware Client Reference*
- *VPN 3002 Hardware Client Quick Start Card*

RQS Nº 03/2005 - CN
CPMI - CORREIOS
27
0437
Fls:
Doc: 3701

Service and Support

For service and support for a product purchased from a reseller, contact the reseller, who offers a wide variety of Cisco service and support programs described in "Service and Support" in *Cisco Information Packet* shipped with your product.

Note If you purchased your product from a reseller, you can access CCO as a guest. CCO is Cisco Systems' primary real-time support channel. Your reseller offers programs that include direct access to CCO services.

For service and support for a product purchased directly from Cisco, use CCO.

Software Configuration Tips on the Cisco TAC Home Page

The Cisco TAC home page includes technical tips and configuration information for the VPN 3000 Concentrator and client. Find this information at:

http://www.cisco.com/warp/public/707/#vpn3000.

Obtaining Documentation

Cisco provides several ways to obtain documentation, technical assistance, and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation on the World Wide Web at this URL:

http://www.cisco.com/univercd/home/home.htm

You can access the Cisco website at this URL:

http://www.cisco.com

International Cisco websites can be accessed from this URL:

http://www.cisco.com/public/countries_languages.shtml

Documentation CD-ROM

Cisco documentation and additional literature are available in a Cisco Documentation CD-ROM package, which may have shipped with your product. The Documentation CD-ROM is updated regularly and may be more current than printed documentation. The CD-ROM package is available as a single unit or through an annual or quarterly subscription.

Registered Cisco.com users can order a single Documentation CD-ROM (product number DOC-CONDOCCD=) through the Cisco Ordering tool:

http://www.cisco.com/en/US/partner/ordering/ordering_place_order_ordering_tool_launch.html

All users can order monthly or quarterly subscriptions through the online Subscription Store:

http://www.cisco.com/go/subscription

Ordering Documentation

You can find instructions for ordering documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/es_inpck/pdi.htm

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Networking Products MarketPlace:

  http://www.cisco.com/en/US/partner/ordering/index.shtml

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, U.S.A.) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

RQS Nº 03/2005 - CN
CPMI - CORREIOS
29
0438
Fls:
Doc: 3701

Documentation Feedback

You can submit comments electronically on Cisco.com. On the Cisco Documentation home page, click **Feedback** at the top of the page.

You can e-mail your comments to bug-doc@cisco.com.

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Obtaining Technical Assistance

Cisco provides Cisco.com, which includes the Cisco Technical Assistance Center (TAC) website, as a starting point for all technical assistance. Customers and partners can obtain online documentation, troubleshooting tips, and sample configurations from the Cisco TAC website. Cisco.com registered users have complete access to the technical support resources on the Cisco TAC website, including TAC tools and utilities.

Cisco.com

Cisco.com offers a suite of interactive, networked services that let you access Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world.

Cisco.com provides a broad range of features and services to help you with these tasks:

- Streamline business processes and improve productivity
- Resolve technical issues with online support
- Download and test software packages
- Order Cisco learning materials and merchandise

- Register for online skill assessment, training, and certification programs

To obtain customized information and service, you can self-register on Cisco.com at this URL:

http://tools.cisco.com/RPF/register/register.do

Technical Assistance Center

The Cisco TAC is available to all customers who need technical assistance with a Cisco product, technology, or solution. Two types of support are available: the Cisco TAC website and the Cisco TAC Escalation Center. The type of support that you choose depends on the priority of the problem and the conditions stated in service contracts, when applicable.

We categorize Cisco TAC inquiries according to urgency:

- Priority level 4 (P4)—You need information or assistance concerning Cisco product capabilities, product installation, or basic product configuration. There is little or no impact to your business operations.
- Priority level 3 (P3)—Operational performance of the network is impaired, but most business operations remain functional. You and Cisco are willing to commit resources during normal business hours to restore service to satisfactory levels.
- Priority level 2 (P2)—Operation of an existing network is severely degraded, or significant aspects of your business operations are negatively impacted by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.
- Priority level 1 (P1)—An existing network is "down," or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Cisco TAC Website

The Cisco TAC website provides online documents and tools to help troubleshoot and resolve technical issues with Cisco products and technologies. To access the Cisco TAC website, go to this URL:

http://www.cisco.com/tac

RQS Nº 03/2005 - CN
CPMI - CORREIOS
31
0439
Fls:
Doc: 3701

All customers, partners, and resellers who have a valid Cisco service contract have complete access to the technical support resources on the Cisco TAC website. Some services on the Cisco TAC website require a Cisco.com login ID and password. If you have a valid service contract but do not have a login ID or password, go to this URL to register:

http://tools.cisco.com/RPF/register/register.do

If you are a Cisco.com registered user, and you cannot resolve your technical issues by using the Cisco TAC website, you can open a case online at this URL:

http://www.cisco.com/tac/caseopen

If you have Internet access, we recommend that you open P3 and P4 cases online so that you can fully describe the situation and attach any necessary files.

Cisco TAC Escalation Center

The Cisco TAC Escalation Center addresses priority level 1 or priority level 2 issues. These classifications are assigned when severe network degradation significantly impacts business operations. When you contact the TAC Escalation Center with a P1 or P2 problem, a Cisco TAC engineer automatically opens a case.

To obtain a directory of toll-free Cisco TAC telephone numbers for your country, go to this URL:

http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml

Before calling, please check with your network operations center to determine the Cisco support services to which your company is entitled: for example, SMARTnet, SMARTnet Onsite, or Network Supported Accounts (NSA). When you call the center, please have available your service agreement number and your product serial number.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- The *Cisco Product Catalog* describes the networking products offered by Cisco Systems, as well as ordering and customer support services. Access the *Cisco Product Catalog* at this URL:

http://www.cisco.com/en/US/products/products_catalog_links_launch.html

- Cisco Press publishes a wide range of networking publications. Cisco suggests these titles for new and experienced users: *Internetworking Terms and Acronyms Dictionary, Internetworking Technology Handbook, Internetworking Troubleshooting Guide,* and the *Internetworking Design Guide.* For current Cisco Press titles and other information, go to Cisco Press online at this URL:

  http://www.ciscopress.com

- *Packet* magazine is the Cisco quarterly publication that provides the latest networking trends, technology breakthroughs, and Cisco products and solutions to help industry professionals get the most from their networking investment. Included are networking deployment and troubleshooting tips, configuration examples, customer case studies, tutorials and training, certification information, and links to numerous in-depth online resources. You can access *Packet* magazine at this URL:

  http://www.cisco.com/go/packet

- iQ Magazine is the Cisco bimonthly publication that delivers the latest information about Internet business strategies for executives. You can access iQ Magazine at this URL:

  http://www.cisco.com/go/iqmagazine

- Internet Protocol Journal is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

  http://www.cisco.com/en/US/about/ac123/ac147/about_cisco_the_internet_protocol_journal.html

- Training—Cisco offers world-class networking training. Current offerings in network training are listed at this URL:

  http://www.cisco.com/en/US/learning/le31/learning_recommended_training_list.html

---

This document is to be used in conjunction with the documents listed in the "Related Documentation" section.

CCIP, CCSP, the Cisco Arrow logo, the Cisco *Powered* Network mark, the Cisco Systems Verified logo, Cisco Unity, Follow Me Browsing, FormShare, iQ Net Readiness Scorecard, Networking Academy, and ScriptShare are

RQS Nº 03/2005 - CN - CPMI - CORREIOS
33
0440
Fls:
3701
Doc:

AP AV

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0441
Fls:
Doc: 3701

3884

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

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0448
Fls:
Doc: 3784

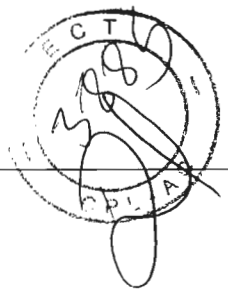
CISCO-FRAME-RELAY-MIB
CISCO-FTP-CLIENT-MIB
CISCO-VOICE-IF-MIB
CISCO-H323-TC-MIB
CISCO-VPDN-MGMT-MIB
CISCO-HSRP-EXT-MIB
DIAL-CONTROL-MIB
RFC1315-MIB
CISCO-HSRP-MIB
ENTITY-MIB
RFC1381-MIB
CISCO-IETF-ATM2-PVCTRAP-MIB
HC-RMON-MIB
CISCO-ISDNU-IF-MIB
RFC1382-MIB
CISCO-IMAGE-MIB
IF-MIB
CISCO-STACKMAKER-MIB
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

© 1992-2003 Cisco Systems, Inc. All rights reserved. Important Notices, Privacy Statement, and Trademarks of Cisco Syste

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0443
Fls:
Doc: 3701

AP AX

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0444
Fls:
Doc: 3701



trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, The Fastest Way to Increase Your Internet Quotient, and iQuick Study are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherSwitch, Fast Step, GigaStack, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, LightStream, MGX, MICA, the Networkers logo, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, RateMUX, Registrar, SlideCast, SMARTnet, StrataView Plus, Stratm, SwitchProbe, TeleRouter, TransPath, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0403R)

Copyright © 2003 Cisco Systems, Inc. All rights reserved.

Cisco 1751 Modular Access Router

The content in this catalog is updated on a monthly basis—for the most current information please see

http://www.cisco.com/en/US/products/hw/routers/ps221/index.html

Product Overview

The 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; and broadband, cable connectivity, and multiservice voice/video/data/fax integration.

The Cisco 1751 router delivers its 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 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 below.

Table 18-30: Cisco 1751 Modular Access Routers

Description	Specification
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, and Cisco IOS IP Plus Voice feature set). Voice and WAN interface cards are available separately.

Key Features and Benefits

Table 18-31: Key Features and Benefits of Cisco 1751

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 Provides a path to migrate to IP Telephony
Modular Architecture	
Accepts an array of WAN and voice interface cards	Adds flexibility and investment protection

ROS Nº 03/2005 - CN
CPML - CORREIOS
0445
Fls:
3701
Doc:

Features	Benefits
WAN interface cards are shared with Cisco 1600, 1700, 2600, and 3600 routers	Reduce cost of maintaining inventory Lower training costs for support personnel Protects 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
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-VPN 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
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	

Features	Benefits
CAR, Policy Routing, WFQ, PQ/CBWFQ, GTS, RSVP, DSCP, cRTP, MLPP 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

For a complete list of physical interfaces, see tables below.

Table 18-32: Physical Interfaces/Architecture

Description	Specification
One 10/100 Base-T 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 18-33: WAN Support

Description	Specification
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 18-34: WAN Interface Cards for the Cisco 1751 Router

Module	Description
WIC-1T	One serial, async, and sync (T1/E1)

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0446
Fls: 3
Doc: 3701

Module	Description
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 10Base-T Ethernet Interface
WIC-1AM	One-port V.90 analog modem WIC
WIC-2AM	Two-port V.90 analog modem WIC
WIC-1SHDSL	One-port G.SHDSL interface

Table 18-35: Voice Interface Cards for the Cisco 1751 Router

Module	Description
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-M1	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-EU]
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
VWIC-1MFT-T1	One-port RJ-48 multiflex trunk—T1
VWIC-2MFT-T1	Two-port RJ-48 multiflex trunk—T1
VWIC-2MFT-T1-D1	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
VWIC-2MFT-E1-D1	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

Voice Implementation Requirements

To implement VoX using the Cisco 1751 router, the following table describes the DSP requirements to support their specific voice port configuration. At a minimum, one DSP is required for each analog VIC and two DSPs for each ISDN BRI VIC.

Table 18-36: DSP resources required based on VIC type

VIC	Number of Voice Calls Supported per VIC	Minimum Number of DSPs Required
Analog (VIC-2FXS, VIC-2FXO, VIC2-E/M)	2	1 DSP (PVDM-256K-4 higher)
Digital (VIC-2BRI-NT/TE)	4 (4 B-channels)	2 DSPs (Two PVDM-256K-4 or one PVDM-256K-8 or higher)
One or two port T1/E1 Multiflex VWICs	24 DS0s for T1 card, 30 DS0s for E1 card [1]	Depends on Codec, refer to table below

1. Cisco 1751 Router supports the maximum 30 DS0 channels.

Table 18-37: 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

The Cisco 1751-V router includes one PVDM-256K-4 (one DSP) which allows support for one analog VIC with no additional DSP requirements. If two analog VICs or one or more digital ISDN VICs are used, then additional DSP resources are needed. The Cisco 1751 router or Cisco 1751-V router has two DSP slots to allow easy expandability to support additional voice channels. For a complete list of DSP modules see table below.

Table 18-38: Cisco 1751 DSP Modules

Module	Description
PVDM-256K-4	4-channel packet voice/fax DSP module (one DSP)
PVDM-256K-8	8-channel packet voice/fax DSP module (two DSPs)
PVDM-256K-12	12-channel packet voice/fax DSP module (three DSPs)
PVDM-256K-16	16-channel packet voice/fax DSP module (four DSPs)
PVDM-256K-20	20-channel packet voice/fax DSP module (five DSPs)

Specifications

Hardware

Table 18-39: Power Specifications for the Cisco 1751

Description	Specification
Locking connector on power socket	Yes
External Power Brick	Yes
AC Input Voltage	100–240 VAC
Frequency	50–60 Hz
AC Input Current	rated 1A, measured 0.5A
Power Dissipation	20W (maximum)

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 0447
3701
Doc:

Table 18-40: Physical and Environmental Specifications for the Cisco 1751

Description	Specification
Dimensions (H x W x D)	4.0 x 11.2 x 8.7 in. (10.0 x 28.4 x 22.1 cm)
Weight (minimum)	3.0 lb (1.36 kg)
Weight (maximum)	3.5 lb (1.59 kg)
Operating Temperature	32 to 104°F (0 to 40°C)
Storage Temperature	–4 to 149°F (–20 to 65°C)
Relative Humidity	10 to 85% noncondensing operating; 5 to 95% noncondensing, nonoperating

Table 18-41: Regulatory Approvals and Certifications for the Cisco 1751

Description	Specification
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

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 below.

Table 18-42: Cisco 1751 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 (see table below). 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 Multicast, 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 18-43: Cisco 1751 Data Software Feature Packs 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=
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=

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 0448
Doc: 3701

Feature Name	Product Code	CD Number
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 Marketing
- Compressed RTP
- Multiple Link PPP & Link Fragmentation and Interleaving
- Resource Reservation Protocol (RSVP)
- Queuing Techniques: Weighted Fair Queuing (WFQ), Priority Queuing (PQ), Low Laterey Queuing (LLQ), and Custom Queuing (CQ)
- Preclassification for IPSec Tunneling
- 802.P

Voice Support

- VoIP
- VoFR
- VoATM

Cisco IOS IP Telephony Features

- Survivable Remote Site Telephony 2.0

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

Ordering Information

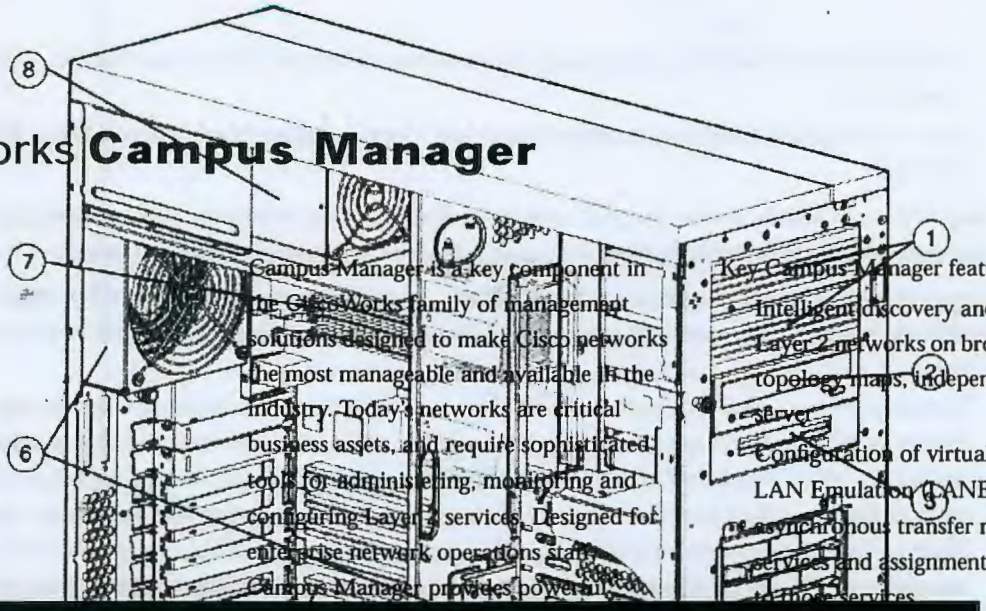
Product Part Numbers

All part descriptions and part numbers for Cisco products can be accessed using the online Cisco Pricing Tool at http://www.cisco.com/cgi-bin/order/pricing_root.pl

The Cisco Pricing Tool requires a user name and password. If you are not already registered, go to http://www.cisco.com/register and follow the instructions. After you have registered, you can access the Pricing Tool.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0449
Fls:
3701
Doc:

CiscoWorks Campus Manager



Campus Manager is a key component in the CiscoWorks family of management solutions designed to make Cisco networks the most manageable and available in the industry. Today's networks are critical business assets, and require sophisticated tools for administering, monitoring and configuring Layer 2 services. Designed for enterprise network operations staff, Campus Manager provides powerful

[redacted]

business and mission-critical systems. The requirement to understand, monitor, and react to changing networking conditions drives the need for sophisticated, yet easy-to-use management tools. Campus Manager is part of the LAN Management Solution, part of the broad range of CiscoWorks network management solutions.

New in Version 3.3:

In addition to the rich set of management features already included, the new version of Campus Manager has been enhanced to provide even greater manageability for Cisco networks. New benefits include:

- Improved application performance
- Doubled capacity for tracking end users

Key Campus Manager features include:

- Intelligent discovery and display of Layer 2 networks on browser-accessible topology maps, independent of VTP server
- Configuration of virtual LAN (VLAN)/ LAN Emulation (LANE) and asynchronous transfer mode (ATM) services and assignment of switch ports to those services

display based
Management
ng
2 configuration

nnectivity related
stations, and
Layer 2 and Layer 3 devices

- Automatic location and correlation of information on users by media access control (MAC), IP address, NT or NetWare Directory Services (NDS) login or UNIX host name, with their physical connections to the switched network
- Visibility and launch point of Cisco CallManager from topology services as well as tracking of phone handset to IP, Mac address, and switch port
- Layer 2 and Layer 3 path trace between source and destination handsets
- Export of topology maps to Visio
- Java plugins to improve graphical user interface (GUI) performance

Cisco Systems, Inc.
All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0450
Fls:
3701
Doc:

- Ability to form Custom Groups in Topology View based on criteria like SysLocation, SysName and IP address/ Subnet mask.
- Secure communication between the client browser and Campus applications using Secure Socket Layer (SSL) protocol.

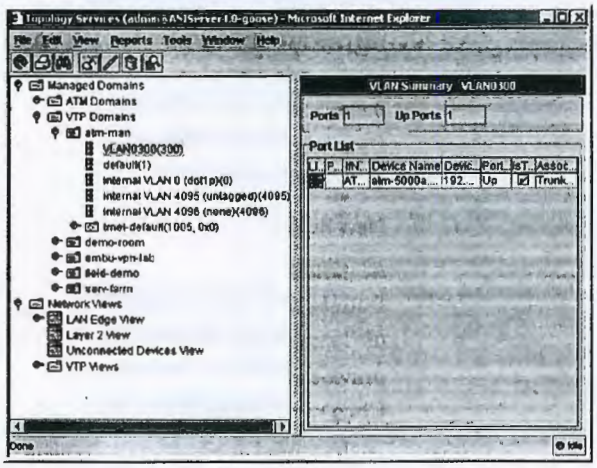
Campus Manager enables administrators to more easily change, monitor, and control network relationships, making them more effective in delivering business-critical and advanced networking services to their users and customers.

Campus Manager is a suite of applications launched from a common "management desktop" used by all Web-based CiscoWorks applications. Campus Manager contains three applications that can be launched from the client's browser:

- Topology Services—This is the principal interface to a variety of large scale topology maps, tabular summaries, reports, and configuration services of the Layer 2 network. A directory-like tree interface lists physical Layer 2 and logical, Virtual Trunking Protocol (VTP), and ATM domain views along with table summaries of the devices and interface associated with these views. This tree structure acts as the launching point for topology maps, discrepancy reporting functions, and configuration services. The integrated VLAN and LANE configuration capabilities, ATM soft permanent virtual circuit (PVC) configuration and diagnostic tools, along with physical and logical configuration discrepancy checking reports and highlighting tools are found within the Topology Services menus. It also supports discovery and display of Cisco Customer Response Applications, and reports on services of these devices.

  Ability to form custom groups based on dynamic and static rules for the group membership. System defined groups and user defined grouping can be created by network administrators and users respectively and allows grouping by developing rules based on criteria such as IP address, subnets, SysLocation, SysName, SysContact, Image Version and hostname. A rules editor allows for creating, editing Topology groups and defines rules for membership.

Figure 1
Topology Services Tabular View



All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Figure 2
VTP Domain Topology Map

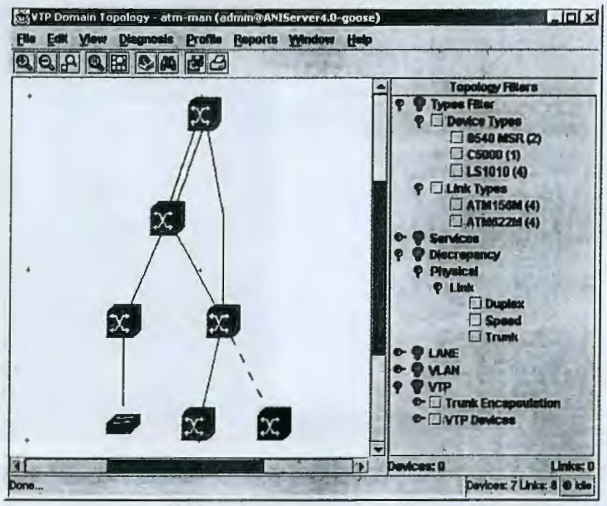
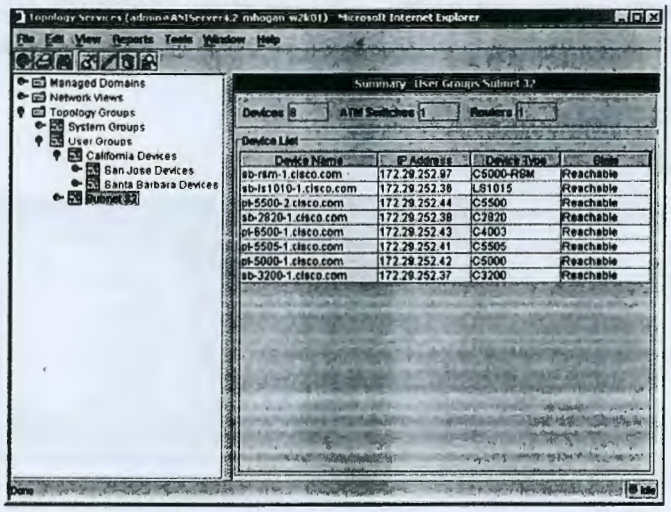


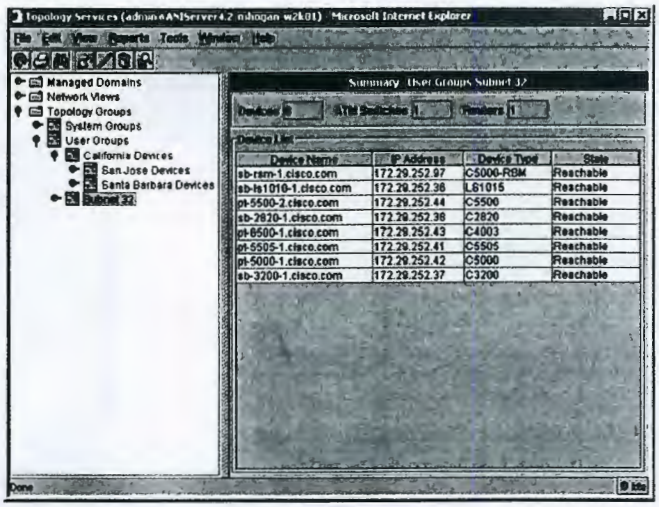
Figure 3
Forming Topology Groups



Cisco Systems, Inc.
All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

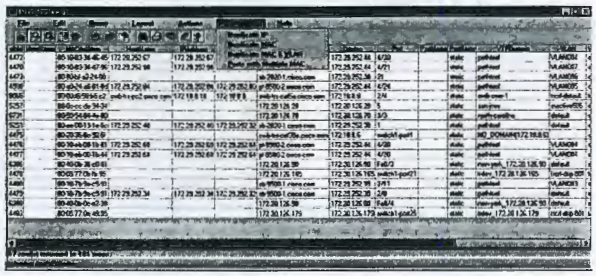
RQS Nº 03/2006 - CN
CPMI - CORREIOS
0451
Fls:
3701
Doc:

Figure 4
Topology Group in Topology Maps



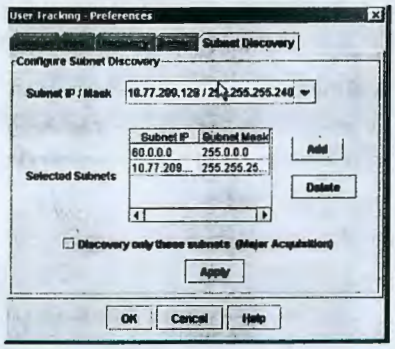
- User Tracking—Designed to assist in locating end-station connections at the access switch, this application is a useful tool in troubleshooting or connectivity analysis. Through automated acquisition, a table of end-user stations and Layer 2 connection information is constructed. This table can be sorted and queried allowing administrators to easily find users. Users can be identified by name, IP handset, MAC and IP address, as well as the switch port and switch that they are connected, along with VLAN and VTP assignment of the port. Predefined reports, such as duplicate MAC per switch port, or duplicate IP addresses, enable managers to locate mobile users or violations in port policies.

Figure 5
User Tracking



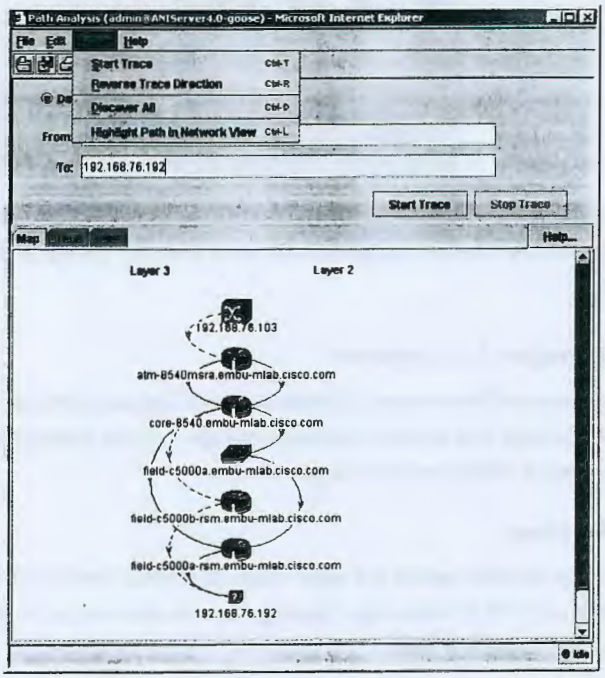
All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Figure 6
Subnet based acquisition



- Path Analysis—An application for switched network management, this is an extremely powerful tool for connectivity troubleshooting. Path Analysis utilizes User Tracking, topology services, and real-time spanning tree information to determine Layer 2 and Layer 3 connectivity between two end-points, or IP Handsets, in the network. The resulting trace is presented in graphical topology views that illustrate the Layer 2 and Layer 3 devices, path direction and link types, and in tabular formats that provide specific interface, IP address, VLAN, and link type information.

Figure 7
Path Analysis



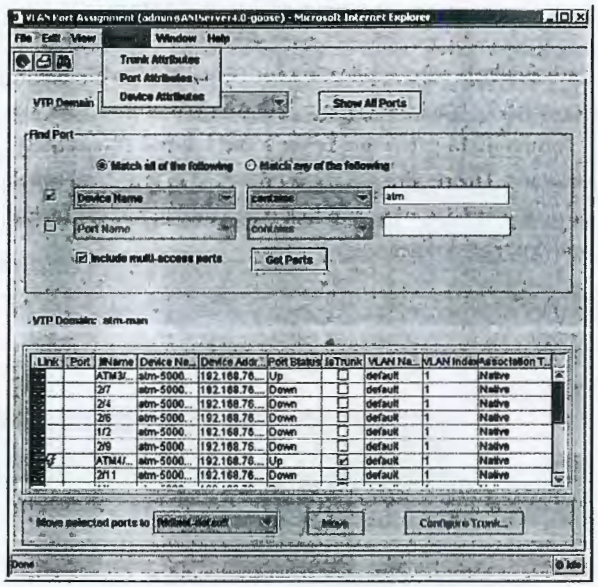
Cisco Systems, Inc.
All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0452
Fls:
3701
Doc:

VLAN/LANE Configuration and Port Assignment

Campus Manager provides an easy and graphical means for creating, modifying, or deleting VLANs, LANE elements, or assigning switch ports to VLANs. As VLANs are created or modified, port and user changes are instantly updated and transmitted to the switches, eliminating the need to update and configure each participating switch individually. As VLANs are selected, the table view shows the participating ports, port status, and switch information and the topology map can be launched to graphically highlight participating devices and links of the VLAN connections. Additional map tools allow managers to show spanning-tree states, VTP trunks, switch port links, and existing LANE service elements.

Figure 8
VLAN Port Assignment



Campus Manager 3.3 is a must for switched network management, and is an integral piece of the LAN Management Solution, by providing a broad, comprehensive set of tools for managing and administering the entire LAN environment.

Campus Manager 3.3 Features

Campus Manager provides a variety of functions within Topology Services, User Tracking, Path Analysis and VLAN/LANE port assignment that network managers can use to better understand, monitor, configure, diagnose, and be proactive to network infrastructure changes.

Topology Services

Topology Services provides access to a wide variety of physical and logical topology maps, summary lists of devices, ports, and their network relationships. Topology Services also acts as the launching point for topology-related configuration and diagnostic tools.

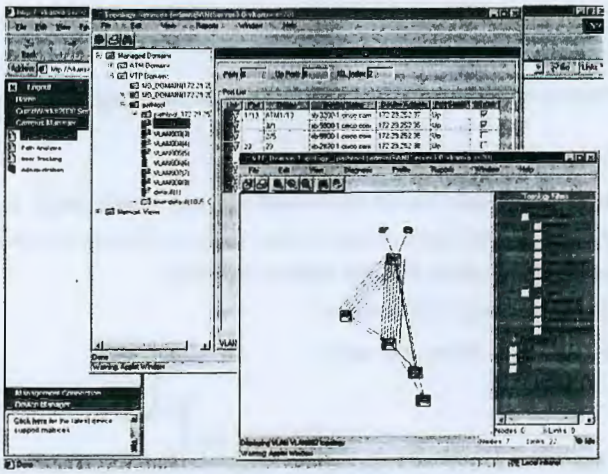
Cisco Systems, Inc.
All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

In Campus Manager 3.3, network topology maps can be displayed in a variety of ways from both a flat Layer 2 to abstracted views that better represent and scale to large campus networks. These abstractions are categorized into three different groups: managed domains, network views and topology groups. Managed domains are topological views of logical groups of devices organized around ATM switch fabrics and VTP domains. Network views are physical displays of the network and are organized to provide full and abstracted views, such as LAN edge views, Layer 2 views, unconnected device views, and VTP views. Topology Groups are custom views that are a subset of the entire network based on the group rule defined while creating the view. They are can be two types of groups—system defined groups that are custom views created by admin user and user defined views which are created by CiscoWorks users. Membership to these groups are made via rules that can be evaluated either automatically or upon user request and these groups help in generating custom views that are a subset of the Layer 2 views.

Key features in the Campus Manager topology services include:

- Autodiscovery and display of Cisco switches, routers, and probes using the Cisco Discovery Protocol (CDP) and SNMP
- Display of physical and logical Layer 2 connections within the discovered LAN environment
- Highlighting tools to identify specific classes of devices or links such as switches, route switch modules (RSMs), Fast Ethernet, EtherChannel®, ATM links, Cisco Customer Response Applications, and other relevant Cisco device elements
- Expanded scalability to support more than 2000 Cisco devices
- Display of multilayer switches and components (switching entities and route-processing entities) with the ability to highlight logical relationships between devices, such as flow masks and shortcuts
- Device status indicators on the topology maps based on CDP, ILMI, ELMI, and SNMP availability
- Automated discrepancy reporting during discovery highlights connection problems, link mismatches, and logical misconfigurations
- Graphical interface for creating VLAN and LANE services for Ethernet, Token Ring, and transparent VLANs
- Graphical interface for locating—through search parameters—and assigning switch ports individually or in bulk to a VLAN
- ATM soft PVC configuration and diagnostics

Figure 9
Topology Views and Tools



Cisco Systems, Inc.
All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS Nº 03/2005 - CN
GPMI - CORREIOS
0453
Fls:
3701
Doc:

VLAN/LANE Configuration and Port Assignment

Campus Manager provides an easy and graphical means for creating, modifying, or deleting VLANs, LANE elements, or assigning switch ports to VLANs. As VLANs are created or modified, port and user changes are instantly updated and transmitted to the switches, eliminating the need to update and configure each participating switch individually. As VLANs are selected, the table view shows the participating ports, port status, and switch information and the topology map can be launched to graphically highlight participating devices and links of the VLAN connections. Additional map tools allow managers to show spanning-tree states, VTP trunks, switch port links, and existing LANE service elements.

VLAN management services provide:

- Tabular summary views of VLANs shows participating ports, devices, links, and port status information
- Graphical setup of VLANs (including transparent VLANs) and VLAN membership to simplify administration
- Integration of LANE configuration services in VLAN configuration tools for more efficient operational and engineering practices
- A separate interface for administrators to quickly search, using a variety of criteria, and assign selected switch ports, individually or in bulk, to VLANs
- Logical display of VLAN configurations makes it easy to visualize switch connections
- Automated discrepancy reports highlight connection problems and link mismatches
- Automated VLAN membership registration reduces administration and configuration requirements

ATM Management

Campus Manager offers a graphical tool for managing complex ATM networks, simplifying configuration and performance monitoring. ATM networks are displayed on the topology map and the logical VLAN and ATM domain views provide graphical representations of ATM switches and LANE elements. "Drill down" capability allows access to configuration and performance monitoring tools. ATM management functions include:

- Autodiscovery of ATM switches, including switched virtual circuit (SVC) and PVC connections
- Connectivity checking of SVC and PVC connections
- End-to-end virtual circuit path tracing and analysis, which assists in connectivity diagnostics
- LANE troubleshooting and performance analysis
- Quality of service (QoS) templates for simplifying the configuration of typical traffic such as video or constant-bit-rate (CBR)
- Simple configuration of soft PVCs
- ATM remote monitoring (RMON) data collection and analysis

User Tracking

User Tracking automatically locates servers and end-user workstations, and Cisco voice over IP (VoIP) telephone handsets and their connections to Layer 2 Cisco switches. During this discovery process it also tabulates specific connection information about that end station, including:

- VLAN name, type, and VTP domain
- Switch port number, name, and state

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

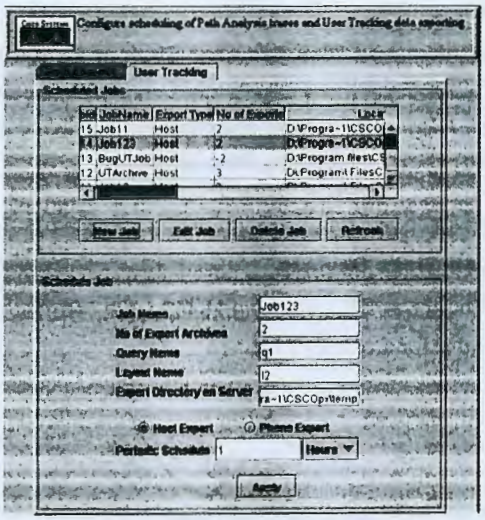
- MAC and IP address of the end station and its subnet
- Tabular and sortable listing of all switch port attached end-user workstations, servers and IP handsets
- Last-seen time stamp reflecting last acquisition in which the end station was detected
- User login name passed automatically from the Windows NT Primary Domain Controller or Novell Directory Structure, or from the UNIX host

Campus Manager simplifies the dynamic nature of many business environments by providing a large number of sortable parameters that can be used to locate end-user stations. User Tracking discovers end stations connected to switch ports automatically and provides a means to identify end users, their assigned VLANs, and host station connections. User Tracking also supports voice/data convergence with interfaces to Cisco CallManager for correlating the IP and MAC addresses of discovered VoIP handsets with their assigned phone number and users.

User Tracking provides the following features:

- Enhanced scalability to support 60,000 end stations
- Predefined reports that identify duplicate MAC and IP addresses, ports with multiple MAC addresses and duplicate sysnames.
- IP and MAC addresses of discovered VoIP handsets with their assigned phone number and users
- Tabular and sortable listing of all switch port-attached end-user workstations and IP handsets
- Customized tables for user-defined, detailed reporting
- GUI for user tracking information table configuration to support dynamic/mobile users
- Scheduling managers for automating address change updates
- Easy-to-use search utility box locating users by MAC addresses, IP addresses, DNS host names, switch port labels, and optional voice handsets
- Provides ability to schedule User Tracking. Also exports User Tracking reports.
- Ability to define acquisition based on a subnet range

Figure 10
Scheduled export of User Tracking Reports



Cisco Systems, Inc.
All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0454
Fls:
Doc: 3701

Path Analysis

Path Analysis is a powerful diagnostic tool for determining the Layer 2 and Layer 3 path between two selected endpoints using Campus Manager-discovered end-station data, VLAN/LANE configuration information, real-time Layer 3 path trace information, and spanning-tree calculations. Displays of path information are available in both topological map and tabular displays. Key Path Analysis features include:

- View the Layer 2 and Layer 3 path information in a map format with traces showing end stations, Layer 2 and 3 devices, route directions, and cut-through paths
- View specific details of the Layer 2 and Layer 3 path, including IP addresses and interfaces traveled, VLAN and VTP domain names, and port speeds and duplex settings
- Perform traces immediately or schedule them
- Perform traces using IP address, DNS name, or by telephone number for voice calls as start/stop points
- Provide Layer 2 and Layer 3 trace information between Cisco voice elements using interfaces to call detail records for specific voice calls
- Provides ability to schedule path traces. Also exports path traces data.

Built on the CiscoWorks Management Server

The CiscoWorks management server provides common resources, such as Web services, discovery, shared databases and database services, and the management desktop. Cisco Management Connection, a service on the CiscoWorks2000 server, delivers a set of tools for integrating applications into the management desktop using Internet-based standards and technologies. These tools allow users to link Web-based management applications to the CiscoWorks family of products and application developers to easily link Web-based applications through a certified registration mechanism. Cisco Management Connection has been used by Cisco and more than 30 network management vendors, including Hewlett-Packard, Computer Associates, Sun Microsystems, and Tivoli Systems to create certified Cisco Management Connections for their applications. This rapid adoption has created an environment in which users can easily build management intranets that link together their favorite Web-based management applications.

Specifications

Server, Client, and Web Browser System Requirements

The server, client and web browser system requirements can be found in the Product Overview documents for the Routed WAN and LAN Management solutions and on Cisco's main on-line documentation site, under each CiscoWorks solution. Please refer to these and other Product Installation documentation for more detailed information on setting up and configuring these solutions.

Supported Cisco Devices

Most Cisco routers, Catalyst® and LightStream switches, as well as Cisco AVVID devices. Contact your Cisco representative for a complete list.

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Supported Cisco IOS Versions

- Cisco IOS® version 10.3 and above
- Catalyst Supervisor code 2.1 and above

Availability

Campus Manager 3.3 is an integral part of multiple CiscoWorks solutions and is not sold as an individual product. For additional information on Campus Manager, see:
http://cisco.com/warp/public/cc/pd/wr2k/

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

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Catalyst, Cisco, Cisco IOS, Cisco Systems, the Cisco Systems logo, and EtherChannel are trademarks or registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0303R)

203046/ETMG_03/05

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0455
Fls:
3701
Doc:

Ap A2

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0456
Fls:
3701
Doc:

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, page 1-1
- Modules, Interface Cards, and Memory, page 1-3
- Memory, page 1-4
- Power Supply Options, page 1-5
- System Specifications, page 1-7
- Regulatory Compliance, page 1-8

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:

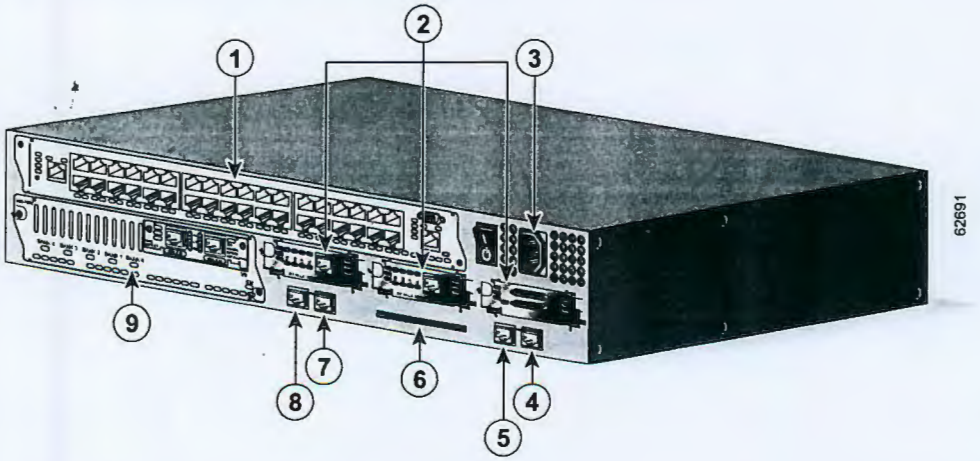
- High-performance 240-MHz Reduced Instruction Set Computer (RISC) processor
- Up to 256 MB SDRAM
- Up to 128 MB Flash memory
- Two slots for network modules, one of which can accommodate a double-width network module
- Three interface card slots

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0457
Fls:
Doc: 3701

- 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

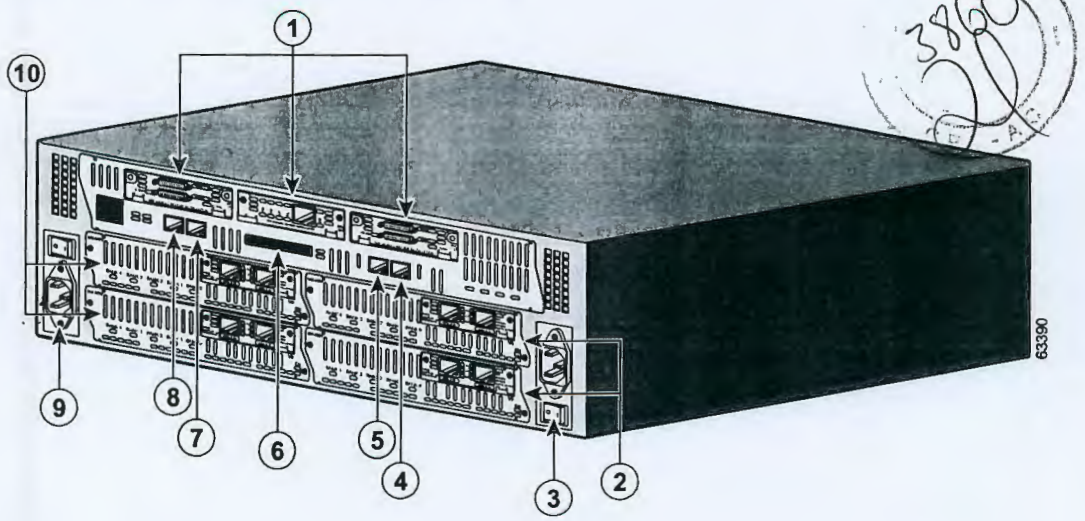
Cisco 3745 routers include the following additional features:

- 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

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 0458
3701
Doc:

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*

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 0459
3701
Doc:

- 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

RQS Nº 03/2005 - CN
CPMI - CORREIOS
01-2180-04
Fls: 0460
Doc: 3701

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.

RQS Nº 03/2005 - CN - CPMI - CORREIOS
Fls: 0461
Doc: 3701

Figure 1-3 Cisco 3725 Router with Optional –48V Power Module Installed

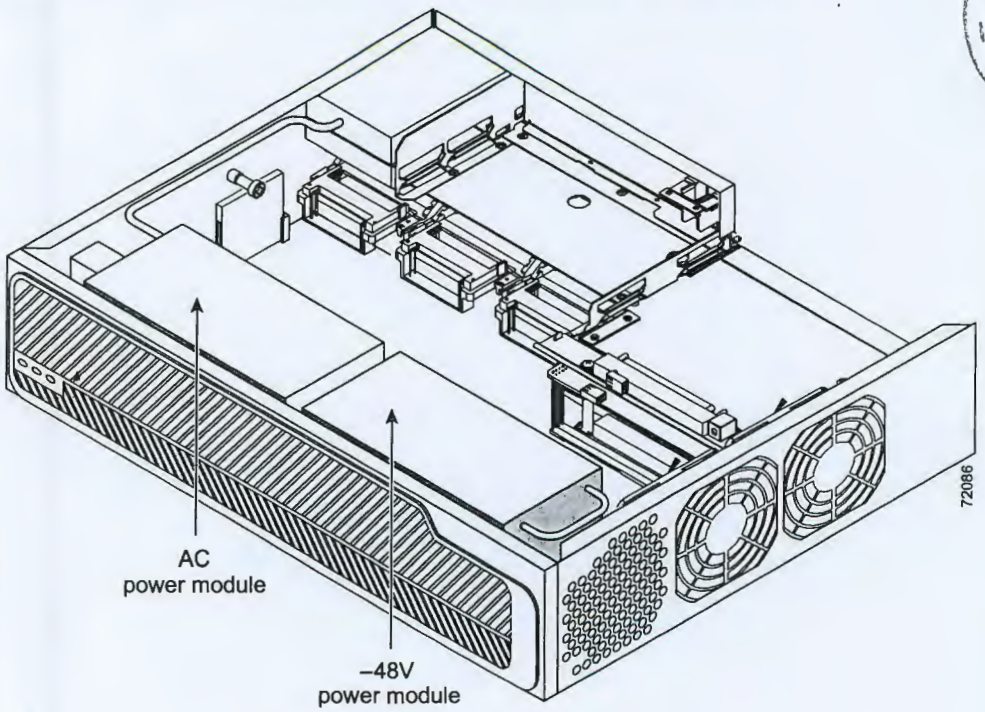
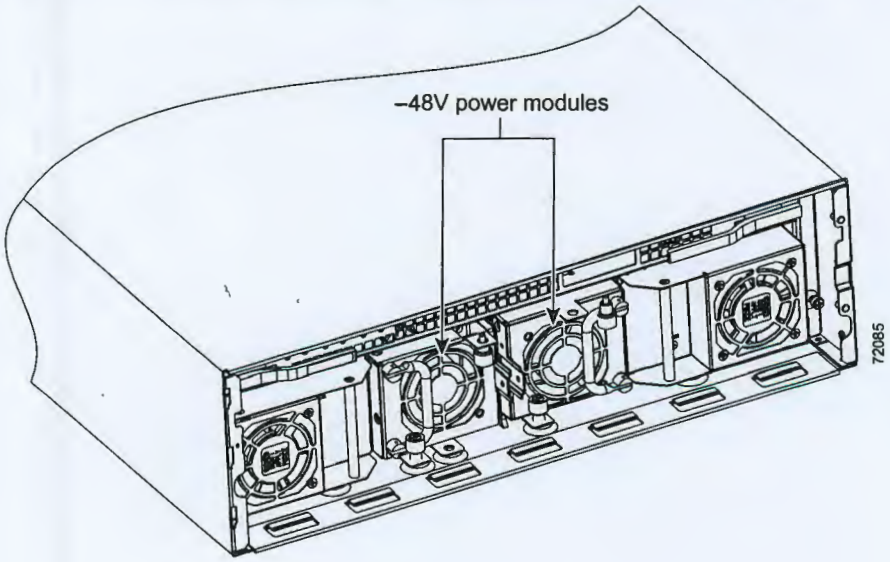


Figure 1-4 Cisco 3745 Router with Optional –48V Power Modules Installed



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

RQS Nº 03/2005 - CN - CPMI - CORREIOS
Fls: 3701
Doc:

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.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0463
Fls:
Doc:

LP BA

RQS Nº 03/2005 - CN
CPMI - CORREIOS

Fls: 0464

Doc: 3701

Cisco Systems

Cisco 3745 Router

1 Cisco 90-Day Limited Hardware Warranty Terms
2 Documents, Equipment, and Tools
3 Install Chassis
4 Connect Cables
5 Power Up the Router
6 Perform Initial Configuration
7 Interface Numbering
8 Where to Go Next
9 Obtaining Documentation
10 Obtaining Technical Assistance
11 Obtaining Additional Publications and Information

CPMI - C
0465
Fls:
3701
Doc:

1 Cisco 90-Day Limited Hardware Warranty Terms

There are special terms applicable to your hardware warranty and various services that you can use during the warranty period. Your formal Warranty Statement, including the warranty applicable to Cisco software, is available on the Cisco Documentation CD and on Cisco.com. Follow these steps to access and download the *Cisco Information Packet* and your warranty document from the CD or from Cisco.com.

1. Launch your browser, and go to this URL:

   http://www.cisco.com/univercd/cc/td/doc/es_inpck/cetrans.htm

   The Warranties and License Agreements page appears.
2. To read the *Cisco Information Packet*, follow these steps:
   a. Click the Information Packet Number field, and make sure that the part number 78-5235-02F0 is highlighted.
   b. Select the language in which you would like to read the document.
   c. Click Go.

      The Cisco Limited Warranty and Software License page from the Information Packet appears.
   d. Read the document online, or click the PDF icon to download and print the document in Adobe Portable Document Format (PDF).

   Note You must have Adobe Acrobat Reader to view and print PDF files. You can download the reader from Adobe's website, http://www.adobe.com.
3. To read translated and localized warranty information about your product, follow these steps:
   a. Enter this part number in the Warranty Document Number field: 78-5236-01C0
   b. Select the language in which you would like to read the document.
   c. Click Go.

      The Cisco warranty page appears.
   d. Review the document online, or click the PDF icon to download and print the document in Adobe Portable Document Format (PDF).

You can also contact the Cisco service and support website for assistance:

http://www.cisco.com/public/Support_root.shtml

Duration of Hardware Warranty

Ninety (90) days.

Replacement, Repair, or Refund Policy for Hardware

Cisco or its service center will use commercially reasonable efforts to ship a replacement part within ten (10) working days after receipt of a Return Materials Authorization (RMA) request. Actual delivery times can vary, depending on the customer location.

Cisco reserves the right to refund the purchase price as its exclusive warranty remedy.

To Receive a Return Materials Authorization (RMA) Number

Contact the company from whom you purchased the product. If you purchased the product directly from Cisco, contact your Cisco Sales and Service Representative.

Complete the information below, and keep it for reference:

Company product purchased from	
Company telephone number	
Product model number	
Product serial number	
Maintenance contract number	

2 Documents, Equipment, and Tools

User Documentation

All the documents described here are available online and on the documentation CD-ROM. To be sure of obtaining the latest information, you should access the online documentation.

To view or print a document in its original page format, access the online document, and click on the PDF icon.

For information about accessing user documentation, see the "Where to Go Next" section on page 20.

Items Included with Cisco 3745 Routers

- Rack-mount brackets; ground lug; power cords
- RJ-45-to-DB-9 adapter cable for console connection
- RJ-45-to-DB-25 adapter cable for modem connection
- Ethernet cables for LAN interface (two)
- *Cisco 2600 Series, 3600 Series, and 3700 Series Regulatory Compliance and Safety Information* document
- *Cisco 3745 Modular Routers Quick Start Guide* (this document)

Items Not Included

Individual items in this list may be required for your particular application:

- Screws for installing the chassis in a rack
- PC running terminal emulation software for administrative access, or modem for remote administrative access
- Cables for WAN and voice interfaces and for additional LAN interfaces
- Tools: Number 2 Phillips screwdriver; ESD-preventive wrist strap

3 Install Chassis

Safety Information

For safety information you need to know before working on your Cisco router, see the *Cisco 2600 Series, 3600 Series, and 3700 Series Regulatory Compliance and Safety Information* document that accompanied this device.

Warning **Only trained and qualified personnel should be allowed to install or replace this equipment.**

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 **To prevent personal injury or damage to the chassis, never attempt to lift or tilt the chassis using the handles on modules (such as power supplies, fans, or cards); these types of handles are not designed to support the weight of the unit.**

ECT 382 CPL-AC

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 0466
Doc: 3701

Installing the Chassis

You can set the chassis on a desktop or install it in a rack. See the applicable instructions that follow.

Rack-Mounting the Chassis

The standard accessory kit contains brackets for mounting the chassis in a 19-inch rack. You can order an optional accessory kit with brackets and instructions for mounting the chassis in a 23- or 24-inch rack.

You can mount the chassis in the following ways:

- Front panel forward
- Rear panel forward
- Center mount with either front or rear panel forward

Attaching Brackets

Attach the mounting brackets to the chassis as shown in Figure 1, Figure 2, or Figure 3, using the screws provided in the bracket kit. Attach the second bracket to the opposite side of the chassis. Use a number 2 Phillips screwdriver to install the bracket screws.

Note Some 19-inch racks have power strips on the rear vertical rails that block cable access to power supplies. Be sure to choose an orientation that provides unrestricted access to the rear panel.

Figure 1 Bracket Installation—Front Panel Forward

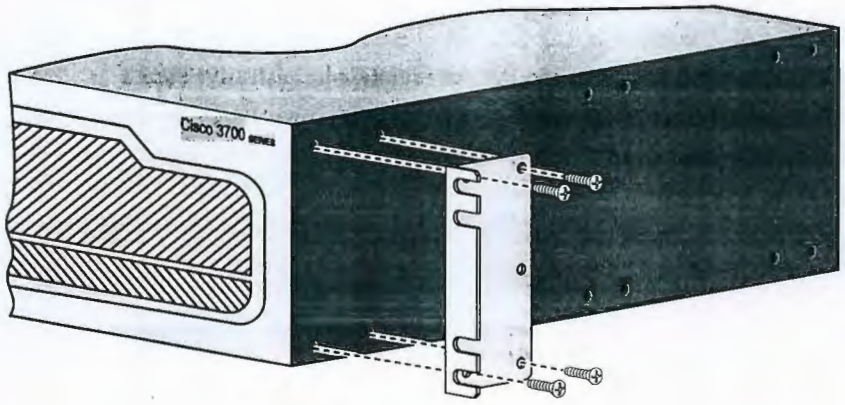


Figure 2 Bracket Installation—Rear Panel Forward

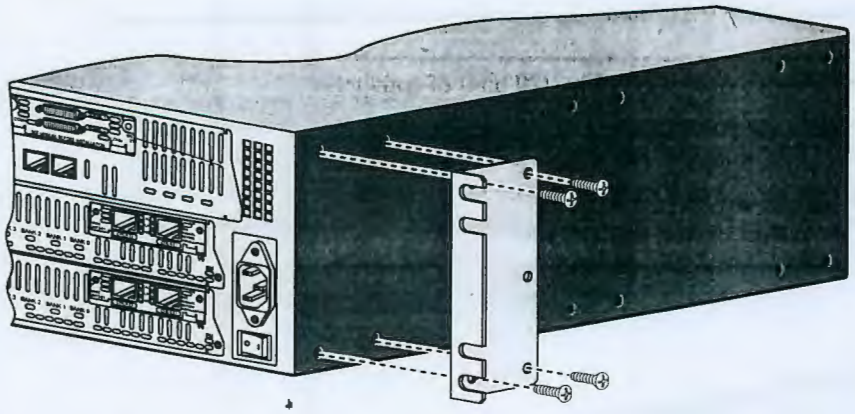
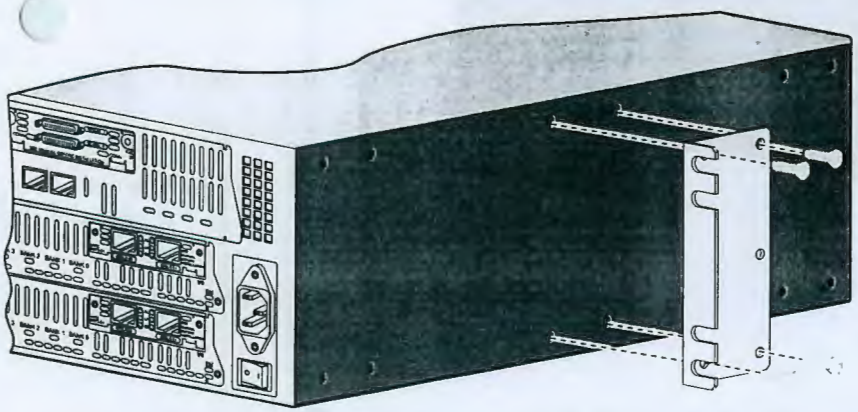


Figure 3 Bracket Installation—Rear Panel Forward, Center-Mount Rack



Note The brackets can also be installed with the front panel forward.

Installing the Chassis in a Rack

In the chassis in the rack. Rack-mounting screws are not provided with the router. Use two screws for each side (supplied with the rack).

Installing on a Desktop

Caution If you place the Cisco 3745 on a desktop, do not place anything on top of the router that weighs more than 10 pounds (4.5 kg). Excessive weight on top could damage the chassis.

ROS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 0467
Doc: 3701

Grounding the Chassis

You must connect the chassis to reliable earth ground using the ground lug (provided) and size AWG 6 (13 mm^2) wire.

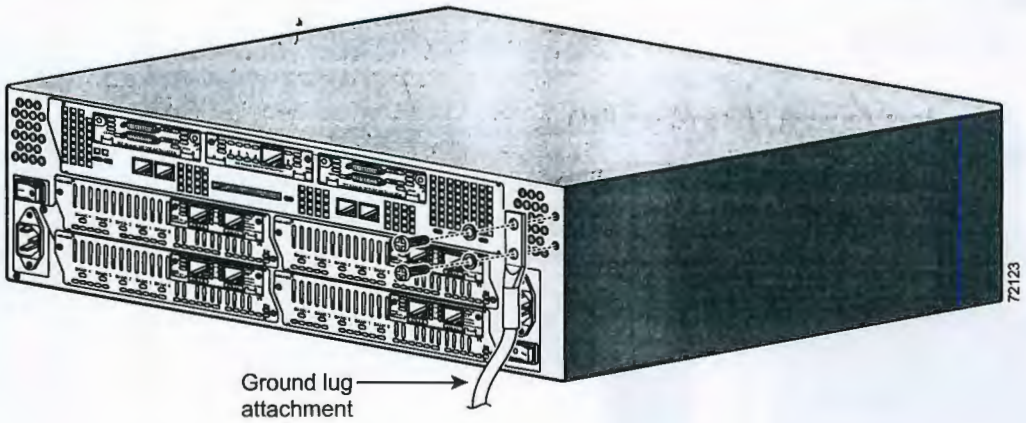
Step 1 Strip one end of the ground wire to expose approximately 0.75 in. (20 mm) of conductor.

Step 2 Use a crimp tool to crimp the ground wire to the ground lug.

Step 3 Attach the ground lug to the chassis as shown in Figure 4. Use a number 2 Phillips screwdriver and the screws supplied with the ground lug. Tighten the screws to a torque of 8 to 10 in-lb (0.9 to 1.1 N-m).

Step 4 Connect the other end of the ground wire to a grounding point at your site.

Figure 4 Required Chassis Ground Connection



4 Connect Cables

Warning **Do not work on the system, or connect or disconnect cables during periods of lightning activity.**

System Management Connections

The connections described in Table 1 provide system management access.

Table 1 System Management Connections

Port	Color	Connected to:	Cable
Console	Light blue	PC or ASCII terminal communication port (usually labeled COM)	RJ-45-to-DB-9 adapter cable
Auxiliary	Black	Modem for remote access	RJ-45-to-DB-25 adapter cable

Power Connections

Connecting Routers to AC Power

If your router uses AC power, connect it to a 15 A, 120 VAC (10 A, 240 VAC) circuit with overcurrent protection.

Note The input voltage tolerance limits for AC power are 85 and 264 VAC.

Warning **AC connected units must have a permanent ground connection in addition to the power cable ground wire. NEBS-compliant grounding satisfies this requirement.**

Warning **This product relies on the building's installation for short-circuit (overcurrent) protection. Ensure that the protective device is rated not greater than:**
15A, 120VAC (10A, 240VAC).

Connecting Routers to DC Power

If your router has a DC-input power supply, follow the directions in this section for proper wiring.

Warning **Before performing any of the following procedures, ensure that power is removed from the DC circuit. To see translations of the warnings that appear in this publication, refer to the *Regulatory Compliance and Safety Information* document that accompanied this device.**

Warning **This product relies on the building's installation for short-circuit (overcurrent) protection. Ensure that the protective device is rated not greater than:**
20A, 60VDC.

Warning **Use copper conductors only.**

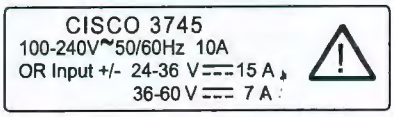
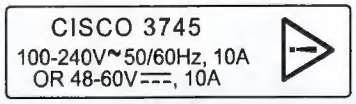
Note The installation must comply with the 1996 National Electric Code (NEC) and other applicable codes.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0468
Fls:
3701
Doc:

DC Wiring Requirements

A Cisco 3745 router with a DC-input power supply requires copper wire for the power connections. Table 2 summarizes the wiring requirements.

Table 2 DC Wiring Requirements for Cisco 3745 Routers

Installed Power Supply	DC Input	DC Input Wire Size	Safety Ground Wire Size	Wire Terminal (Lug)	Overcurrent Protection
Nominal 24/48 VDC[1] Identified by the following printed label: 	24 - 36 V, 15 A	AWG 12 (3.0 mm^2)	AWG 12 (3.0 mm^2), minimum	Amp/Tyco No. 52961 or equivalent	20 A maximum
	36 - 60 V, 7 A	AWG 12 or 14 (3.0 or 2.0 mm^2)	AWG 12 (3.0 mm^2), minimum	For AWG 12: Amp/Tyco No. 52961 or equivalent For AWG 14: Molex No. 19099-0017 or equivalent	20 A maximum
Nominal 48 VDC[2] Identified by the following printed label: 	48 - 60 V, 10 A	AWG 14 or 16 (2.0 or 1.2 mm^2)	AWG 14 (2.0 mm^2), minimum	For AWG 14 or 16: Molex No. 19099-0017 or equivalent	20 A maximum

1. The input voltage tolerance limits for nominal 24/48 V power supplies are 18 and 72 VDC.
2. The input voltage tolerance limits for nominal 48 V power supplies are 38 and 72 VDC.

Wiring Procedure for DC Input

To connect the router to a DC power source, perform the following steps:

Step 1 Remove power from the DC circuit. To ensure that power is removed from the DC circuit, locate the circuit breaker for the DC circuit, switch the circuit breaker to the OFF position, and tape the circuit-breaker switch in the OFF position.

Tip Secure all power cabling when installing this unit to avoid disturbing field-wiring connections.

Step 2 Strip the wires to the appropriate length for the terminals. The strip length is 1/8 to 3/16 inch (3 to 5 mm) for Molex number 19073-0009 terminals and for AMP/Tyco number 52961 terminals.

Step 3 Crimp the terminals onto the DC power input wires.

Warning **When stranded wiring is required, use approved wiring terminations, such as closed-loop or spade-type with upturned lugs. These terminations should be the appropriate size for the wires and should clamp both the insulation and conductor.**

Step 4 Remove the plastic cover from the terminal block. Save it for reinstallation after you finish wiring.

Step 5 Connect the DC power input wires to the terminal block as shown in Figure 5 or Figure 6.

Caution Do not overtorque the terminal block screws. The recommended torque is 8.0 ± 0.5 in-lb (0.93 ± 0.05 N-m).

Figure 5 *Terminal Block Connections for Negative Polarity DC Input Power*

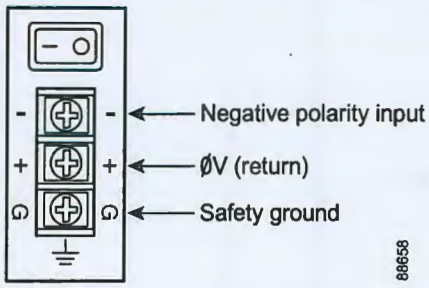
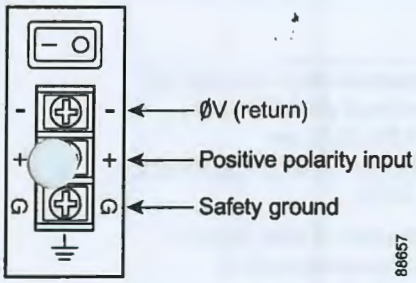


Figure 6 *Terminal Block Connections for Positive Polarity DC Input Power*



Step 6 Install the plastic cover over the terminal block.

Warning **The safety cover is an integral part of the product. Do not operate the unit without the safety cover installed. Operating the unit without the cover in place will invalidate the safety approvals and pose a risk of fire and electrical hazards.**

Step 7 Secure the wires using cable ties.

Step 8 If your router has a second power supply installed, repeat Step 1 through Step 7 for the second power supply.

Step 9 Turn on power to the DC circuit.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 0469
Doc: 3701

WAN, LAN, and Voice Connections

The connections and cables listed here are described in detail in the following documents:

- *Cisco 3700 Series Hardware Installation Guide*
- *Cisco Network Modules Hardware Installation Guide*
- *Cisco Interface Cards Installation Guide*
- *Cisco Modular Access Router Cable Specifications*

For information about accessing these documents, see the "Where to Go Next" section on page 20.

Table 3 summarizes some typical WAN, LAN, and voice connections for Cisco 3745 routers.

Table 3 WAN, LAN, and Voice Connections

Port or Connection	Port Type, Color	Connected to:	Cable
FastEthernet	RJ-45, yellow,	Ethernet hub or switch	Straight-through Ethernet
T1/E1 WAN	RJ-48C/CA81A, blue	T1 or E1 network	RJ-48 T1
Cisco serial	60-pin D-sub	CSU/DSU and serial network or equipment	Cisco serial transition cable that matches the signaling protocol (EIA/TIA-232, EIA/TIA-449, V.35, X.21, or EIA/TIA-530) and the serial port operating mode (DTE or DCE). See the *Cisco Modular Access Router Cable Specifications* document for information about selecting these cables.
Cisco Smart serial	Cisco Smart compact connector, blue	CSU/DSU and serial network or equipment For WIC-2T and WIC-2A/S only	
DSL	RJ-11C/CA11A, lavender	Network demarcation device for service provider's DSL interface	RJ-11
T1 digital voice	RJ-48C/CA81A, tan	Digital PBX	RJ-48 T1 cable
Analog voice FXS	RJ-11, gray	Telephone, fax	RJ-11
Analog voice FXO	RJ-11, pink	Central office, analog PBX	RJ-11
Analog voice E&M	RJ-11, brown	Analog PBX	RJ-11
BRI S/T WAN (external NT1)	RJ-48C/CA81A, red	NT1 device or private integrated network exchange (PINX)	RJ-48
BRI U WAN (built-in NT1)	RJ-49C/CA-A11, orange	ISDN network	RJ-49
CT1/PRI	T1	External T1 CSU	DB-15 T1 serial cable
CT1/PRI-CSU	T1	RJ-48C/CA81A interface	RJ-48 straight-through
CE1/PRI	E1	E1 network	DB-15 to BNC, DB-15 to DB-15, DB-15 to twinax, or DB-15 to RJ-45
56/64-kbps DSU/CSU	8-pin modular, blue	RJ-48S interface	RJ-48 straight-through

5 Power Up the Router

Checklist for Power-Up

You are ready to power on the Cisco router if the following steps are completed:

- The chassis is securely mounted.
- Power and interface cables are connected.
- Your PC terminal emulation program is configured for 9600 baud, 8 data bits, 1 stop bit, and no parity.
- You have selected passwords for access control.
- You have determined the IP addresses for the Ethernet and serial interfaces.

Front Panel Indicators

The following indicator LEDs provide power, activity, and status information:

- SYS—System status:
  - Blinking green during boot-up—System is booting
  - Continuous green—System booted and OK
  - Blinking green continuing after boot-up—System is in ROM monitor mode
  - Amber—System malfunction
- ACT—Activity:
  - Blinking or continuous green during system activity, such as interrupts and packet transfers
- SYS PS1 or SYS PS2—Chassis power supply number 1 or number 2 status:
  - Off—Powered off, not installed, or faulty
  - Continuous green—Installed and operating
  - Amber—Installed and powered off or faulty
- –48V PS1 or –48V PS2—IP power module number 1 or number 2 status:
  - Off—Faulty or not installed
  - Continuous green—Installed and operating
  - Amber—Installed and powered off or faulty

Power-Up Procedure

Perform this procedure to power up your Cisco router and verify that it goes through its initialization and self-test. When this procedure is finished, the Cisco router is ready to configure.

Note To view the boot sequence through a terminal session, you must have a console connection to the Cisco router before it powers on.

Move the power switch on the chassis power supply, or on both chassis power supplies, to the ON position.

The fan should operate, and the SYS PS LED should be continuous green for each power supply that is in use. The SYS LED should blink while the system boots, and it should be continuous green after the system boots. If this does not happen, see the power-on procedure in the *Cisco 3700 Series Hardware Installation Guide*.

Note If no Cisco IOS image is loaded on the Cisco 3745, the router enters ROMMON mode, and the system LED blinks.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
11
Fls: 0470
3701
Doc:

Messages begin to appear in your terminal emulation program window.

Caution *Do not press any keys on the keyboard until the messages stop.* Any keys pressed during this time are interpreted as the first command typed when the messages stop, which might cause the router to power off and start over. It takes a few minutes for the messages to stop.

When you see the following messages, the router has booted and is ready for initial configuration. See the following section for initial configuration procedures.

```
        --- System Configuration Dialog ---

At any point you may enter a question mark '?' for help.
Use ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.

Would you like to enter the initial configuration dialog? [yes/no]:
```

Note If the `rommon 1>` prompt appears, your system has booted in ROM monitor mode. For information on the ROM monitor, see the router rebooting and ROM monitor information in the *Cisco IOS Configuration Fundamentals Configuration Gulde* for your Cisco IOS software release.

You can access this document at the locations described in the "Where to Go Next" section on page 20.

6 Perform Initial Configuration

You can configure your router by using one of the following tools:

- Setup Command Facility. See the "Initial Configuration Using Setup Command Facility" section on page 12.
- Security Device Manager (SDM). See the "Initial Configuration Using Security Device Manager" section on page 14.
- Command-Line Interface (CLI). See the "Initial Configuration Using the CLI (Manual Configuration)" section on page 17.

Note If you need help with the interface and port numbering, see the "Interface Numbering" section on page 18.

Initial Configuration Using Setup Command Facility

This section shows how to prepare the system for communication functions through its Ethernet and WAN interfaces.

For a description of the interface numbering, see the "Interface Numbering" section on page 18.

Note If you make a mistake while using the setup command facility, you can exit and run the facility again. Press Ctrl-c, and type setup at the privileged EXEC mode prompt (`3700#`).

Step 1 To proceed using the setup command facility, enter yes.

```
Would you like to enter the initial configuration dialog? [yes/no]: yes
```

Step 2 When the following messages appear, press Return to enter basic management setup:

```
At any point you may enter a question mark '?' for help.
Use ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.

Basic management setup configures only enough connectivity
for management of the system, extended setup will ask you
to configure each interface on the system
```

```
Would you like to enter basic management setup? [yes/no]: yes
```

Step 3 Enter a host name for the router (this example uses 3745):

```
Configuring global parameters:

  Enter host name [Router]: 3745

The enable secret is a password used to protect access to privileged EXEC and configuration modes. This
password, after entered, becomes encrypted in the configuration.
```

Step 4 Enter an enable secret password. This password is encrypted (more secure) and cannot be seen when viewing the configuration:

```
Enter enable secret: xxxx

The enable password is used when you do not specify an enable secret password, with some older software
versions, and some boot images.
```

Step 5 Enter an enable password that is different from the enable secret password. This password is *not* encrypted (less secure) and can be seen when viewing the configuration:

```
Enter enable password: xxxx

The virtual terminal password is used to protect access to the router over a network interface.
```

Step 6 Enter the virtual terminal password, which prevents unauthenticated access to the router through ports other than the console port:

```
Enter virtual terminal password: xxxx
```

Step 7 Respond to the following prompts as appropriate for your network:

```
Configure SNMP Network Management? [yes]: yes
    Community string [public]:
```

Step 8 A summary of the available interfaces is displayed:

Note The interface numbering that appears is dependent on the type of Cisco modular router platform and on the installed interface modules and cards.

```
Current interface summary

Controller Timeslots D-Channel Configurable modes Status
T1 3/0     24         23        pri/channelized    Administratively up
T1 3/1     24         23        pri/channelized    Administratively up

Any interface listed with OK? value "NO" does not have a valid configuration

Interface                IP-Address      OK? Method Status                Protocol
FastEthernet0/0          unassigned      NO  unset  up                    down

FastEthernet0/1          unassigned      NO  unset  up                    down
```

Step 9 Select one of the available interfaces for connecting the router to the management network:

```
Enter interface name used to connect to the
management network from the above interface summary: fastethernet0/0
```

Step 10 Respond to the following prompts as appropriate for your network:

```
Configuring interface FastEthernet0/0:
  Use the 100 Base-TX (RJ-45) connector? [yes]:
  Operate in full-duplex mode? [no]: yes
  Configure IP on this interface? [yes]:
    IP address for this interface: 10.1.1.1
    Subnet mask for this interface [255.0.0.0] : 255.255.0.0
    Class A network is 10.0.0.0, 16 subnet bits; mask is /16
```

RQS Nº 03/2005 - CN
CPMI - CORREIOS
13
0471
Fls:
Doc: 3701

Step 11 After the following messages appear, press Return to save the basic configuration:

```
The following configuration command script was created:

hostname 3745
enable secret 5 $1$Ksjf$za4T2lb3ARS5d1PHVzW5A0
enable password xxxx
line vty 0 4
password xxxx
snmp-server community public
!
no ip routing

!
interface FastEthernet0/0
no shutdown
media-type 100BaseX
full-duplex
ip address 10.1.1.1 255.255.0.0
!
interface FastEthernet0/1
shutdown
no ip address
!
end


[0] Go to the IOS command prompt without saving this config.
[1] Return back to the setup without saving this config.
[2] Save this configuration to nvram and exit.

Enter your selection [2]: 2


Press RETURN to get started! RETURN
```

Step 12 The user prompt is displayed.

```
3745>
```

When you have completed the basic configuration tasks, your Cisco router is ready to configure for specific functions. See the "Where to Go Next" section on page 20 for information about locating documentation for advanced configuration procedures.

Initial Configuration Using Security Device Manager

Security Device Manager (SDM) is a web-based configuration tool that allows you to configure LAN and WAN interfaces, routing, Network Address Translation (NAT), firewalls, Virtual Private Networks (VPNs), and other features on your router. SDM runs on a PC connected to the router through an Ethernet or FastEthernet interface, and it requires a web browser, either Internet Explorer version 5.5 or later or Netscape version 4.79. SDM is compatible with Microsoft Windows 2000, Windows NT 4.0 (with Service Pack 4), Windows 98, Windows ME, and Microsoft Windows XP.

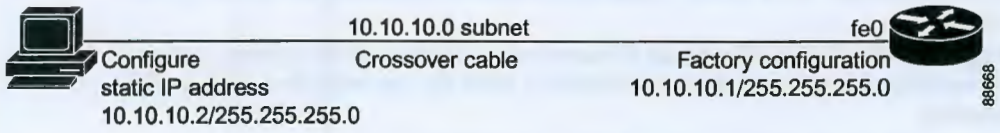
This procedure applies to routers that have the SDM configuration tool preinstalled.

To configure your router by using SDM, first assign an IP address to the Ethernet port of the PC as directed in the "Assign a Static IP Address to the PC" section, and then start SDM as described in the "Start SDM" section on page 15.

Assign a Static IP Address to the PC

Assign a static IP address in the 10.10.10.0 subnet to the Ethernet port of the PC, as shown in Figure 7. The recommended IP address for this interface is 10.10.10.2. The FastEthernet 0/0 interface of the router is preconfigured with the IP address 10.10.10.1.

Figure 7 Initial IP Addresses in the 10.10.10.0 Subnet for SDM



Start SDM

To start SDM and begin the router configuration, perform the following procedure:

Step 1 Connect the Ethernet port of the PC to the FastEthernet 0/0 port of the router, using a crossover cable.

Step 2 Open a web browser on the PC, and enter the following URL:

https://10.10.10.1/flash/sdm.shtml

Note https://... specifies that the Secure Socket Layer (SSL) protocol is used for a secure connection. If SSL is not available, you can use http://... .

Step 3 Enter the username sdm and the password sdm in the dialog box.

Step 4 A window appears informing you that Verisign certifies that this is a Cisco application. Click Yes, or click Grant to accept the certificate and proceed. Additional certificate windows appear if you are using Netscape; click Grant to accept the certificates.

The SDM Launch page appears after a short time. (See Figure 8.) Leave this window open and wait for the next window.

Figure 8 SDM Launch Page

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0472
Fls:
Doc: 3701

Tip If the SDM Launch page does not appear when you enter the URL https://10.10.10.1/flash/sdm.shtml, test the connection between the PC and the router by doing the following:

a. Check that the POWER LED on the router is on and that the ACTIVITY LED is on, indicating an active Ethernet connection between the router and the PC. If the ACTIVITY LED is not on, verify that you are using a crossover cable to connect the PC to the router.

b. If the Launch page still does not appear, verify that the web browser's "work offline" option is disabled. In Internet Explorer, click the File menu, and verify that the "work offline" option is unchecked. In Netscape, the default selection in the File menu is set to "work online."

c. If the Launch page still does not appear, verify that the file sdm.tar is loaded into the router's Flash memory. Open a Telnet session to 10.10.10.1, entering the username sdm and the password sdm. Enter the command show flash to verify that sdm.tar is loaded in Flash memory.

d. If the web page still does not appear, verify that the PC is configured with a static IP address.

Step 5 A window appears with information about the web browser and its settings. This window also informs you that SDM will open in another window. Close this window and wait for the SDM Startup Wizard page to appear.

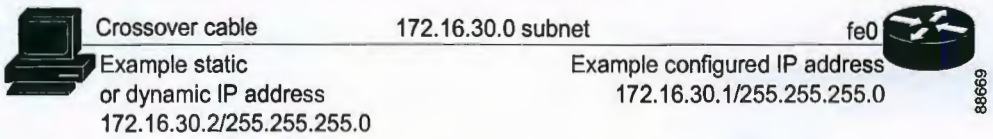
Step 6 When the SDM Startup wizard appears, click Next to begin. Use the wizard to give the router a hostname, to assign a login username and password, to set an enable secret password, and to assign a new LAN IP address to the FastEthernet interface 0/0. You can also configure the router as a Dynamic Host Configuration Protocol (DHCP) server, identify Domain Name System (DNS) and Windows Internet Naming Service (WINS) servers, and make security settings.

Tip Be sure to write down the enable secret password. It is not revealed in the summary window and cannot be recovered.

Step 7 When the Summary window appears, write down the LAN IP address, hostname, login username, and user password that you entered, and click Finish. (You will need this information to reconnect to the router and use SDM to perform additional configuration.)

Step 8 Assign a new IP address to the PC's Ethernet interface; place it on the same subnet as the router's FastEthernet 0/0 port, which you assigned in Step 6 above. (See Figure 9.) If you configured a DHCP server on the router, configure the PC to obtain an IP address automatically. The IP addresses in Figure 9 are examples only.

Figure 9 IP Addresses in the Renumbered Subnet for SDM



Step 9 Open a web browser on the PC, and enter the SDM URL, using the new IP address that you gave the LAN interface: https://*new-IP-address*/flash/sdm.shtml. In the example shown in Figure 9, you would enter `https://172.16.30.1/flash/sdm.shtml`.

Step 10 Enter the username and password that you specified in Step 6 above.

Step 11 When the SDM System Overview window appears, you can use the wizard buttons on the left side of the window to configure other features. Buttons are provided for LAN, WAN, firewall, and VPN configurations.

For more information about SDM, refer to the *Cisco Security Device Manager Troubleshooting Guide* at the following URL, http://www.cisco.com/go/sdm. See the "Obtaining Documentation" section on page 20 for information about accessing this document.

Initial Configuration Using the CLI (Manual Configuration)

This section shows how to bring up a command-line interface (CLI) prompt for configuration using the CLI, and it directs you to the documentation for CLI configuration.

Note To avoid losing work you have completed, be sure to save your configuration occasionally as you proceed. Use the copy running-config startup-config command to save the configuration to NVRAM.

Step 1 To proceed with manual configuration using the CLI, enter no.

```
Would you like to enter the initial configuration dialog? [yes/no]: no
```

Step 2 Press Return to terminate autoinstall and continue with manual configuration.

```
Would you like to terminate autoinstall? [yes] Return
```

Several messages are displayed, ending with a line similar to the following:

```
...
Copyright (c) 1986-2002 by cisco Systems, Inc.
Compiled date time by person
```

Step 3 Press Return to bring up the `Router>` prompt.

```
...
flashfs[4]: Initialization complete.
Router>
```

Step 4 Enter privileged EXEC mode.

```
Router> enable
Router#
```

For configuration using the CLI, refer to the applicable configuration procedures in the *Software Configuration Guide: Cisco 2600 Series, Cisco 3600 Series, and Cisco 3700 Series Routers*. See the "Where to Go Next" section on page 20 for information about accessing this document.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 0473
Doc: 3701

7 Interface Numbering

Each individual interface (port) on a Cisco 3745 router is identified by number as described in the following sections.

WAN and LAN Interface Numbering

The Cisco 3745 router chassis contains the following WAN and LAN interface types:

- 2 built-in FastEthernet LAN interfaces
- 3 slots in which you can install WAN or voice interface cards
- 4 network module slots

The numbering format is:

- *Interface-type Slot-number/Interface-number*

  Two examples are: `FastEthernet 0/0` and `Serial 1/2`.

The slot numbers are as follows:

- 0 for all built-in interfaces
- 0 for all WIC interfaces
- 1 for the lower-right network module slot
- 2 for the lower-left network module slot
- 3 for the upper-right network module slot
- 4 for the upper-left network module slot

If double-width network modules are installed, the network module slots are numbered as follows:

- 2 for the lower double-width slot
- 4 for the upper double-width slot

Interface (port) numbers begin at 0 for each interface type, and continue from right to left and from bottom to top.

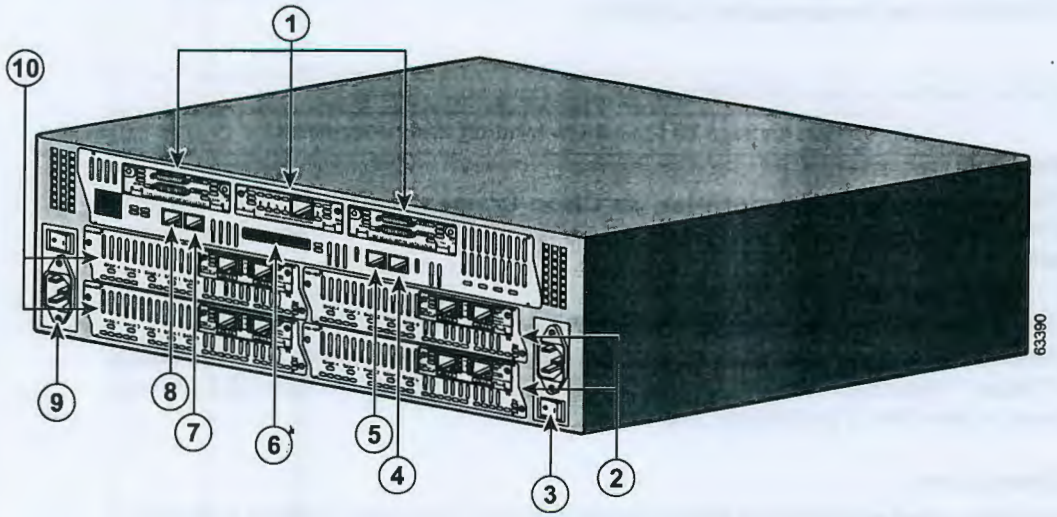
Figure 10 shows the rear panel of the Cisco 3745 with:

- A WIC in each of the three WAN interface card slots
- A single-width network module in each of the four network module slots
- Two AC power supplies

Note The slot number for all WIC interfaces is always 0. (The W0, W1, and W2 slot designations are for physical slot identification only.) Interfaces in the WICs are numbered from right to left, starting with 0/0 for each interface type, regardless of which physical slot the WICs are installed in. Some examples are:

- If physical slot W0 is empty and physical slot W1 contains a 1-port serial WIC, the serial interface in the WIC is numbered Serial 0/0.
- If slot W0 contains a 2-port serial WIC and slot W1 contains a 1-port serial WIC, the serial interfaces in physical slot W0 are numbered Serial 0/0 and Serial 0/1, and the serial interface in physical slot W1 is numbered Serial 0/2.
- If slot W0 contains a 2-port serial WIC and slot W1 contains a 1-port BRI WIC, the serial interfaces in physical slot W0 are numbered Serial 0/0 and Serial 0/1, and the BRI interface in physical slot W1 is numbered BRI 0/0.

Figure 10 Cisco 3745 Rear Panel



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	9	Power supply
5	FastEthernet 0/1	10	Network modules

Voice Interface Numbering

Voice interfaces are numbered differently from the WAN interfaces described in the previous section. Voice interfaces are numbered as follows:

network-module-slot/voice-module-slot/voice-interface

If a 4-channel voice network module is installed in chassis slot 1, the voice interfaces are:

- 1/0/0—Network module slot 1/Voice module slot 0/Voice interface 0
- 1/0/1—Network module slot 1/Voice module slot 0/Voice interface 1
- 1/1/0—Network module slot 1/Voice module slot 1/Voice interface 0
- 1/1/1—Network module slot 1/Voice module slot 1/Voice interface 1

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0474
Fls:
Doc: 3701

8 Where to Go Next

For additional detailed configuration procedures, refer to the appropriate Cisco 3700 series documentation or Cisco IOS software documentation, available on-line and on the Documentation CD-ROM:

Tip See the "Obtaining Documentation" section on page 20 for help in locating these documents.

To access Cisco 3700 series platform documentation on Cisco Connection Online (CCO):

On the Cisco.com home page at http://www.cisco.com, locate the Technical Documentation tab, and click on "Locate Technical Documentation on Cisco Connection Online." Under the Product Documentation heading, navigate to Modular Access Routers and to the documentation for your router.

To access Cisco IOS software documentation on Cisco Connection Online (CCO):

On the Cisco.com home page at http://www.cisco.com, locate the Technical Documentation tab, and click on "Locate Technical Documentation on Cisco Connection Online." Under the Product Documentation heading, navigate to the Cisco IOS software documentation for the Cisco IOS software release that is installed on your router.

To access documentation on Cisco.com:

For Cisco 3700 series platform documentation, start on Cisco.com at http://www.cisco.com, and select Products & Services > Routers > Cisco 3700 Series Multiservice Platforms > Technical Documentation > *Document type* > *Document.*

For Cisco IOS software documentation, start on Cisco.com at http://www.cisco.com, and select Products & Services > IOS Software > Cisco IOS Software Releases > *Your Cisco IOS software release.*

To get updated information about platform support for features, select Feature Navigator II, if you have an account on Cisco.com. You can also access Feature Navigator II at http://www.cisco.com/go/fn.

9 Obtaining Documentation

Cisco provides several ways to obtain documentation, technical assistance, and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation on the World Wide Web at this URL:

http://www.cisco.com/univercd/home/home.htm

You can access the Cisco website at this URL:

http://www.cisco.com

International Cisco websites can be accessed from this URL:

http://www.cisco.com/public/countries_languages.shtml

Documentation CD-ROM

Cisco documentation and additional literature are available in a Cisco Documentation CD-ROM package, which may have shipped with your product. The Documentation CD-ROM is updated regularly and may be more current than printed documentation. The CD-ROM package is available as a single unit or through an annual or quarterly subscription.

Registered Cisco.com users can order a single Documentation CD-ROM (product number DOC-CONDOCCD=) through the Cisco Ordering tool:

http://www.cisco.com/en/US/partner/ordering/ordering_place_order_ordering_tool_launch.html

All users can order monthly or quarterly subscriptions through the online Subscription Store:

http://www.cisco.com/go/subscription

Ordering Documentation

You can find instructions for ordering documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/es_inpck/pdi.htm

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Networking Products MarketPlace:

  http://www.cisco.com/en/US/partner/ordering/index.shtml
- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, U.S.A.) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

You can submit comments electronically on Cisco.com. On the Cisco Documentation home page, click Feedback at the top of the page.

You can e-mail your comments to bug-doc@cisco.com.

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

10 Obtaining Technical Assistance

Cisco provides Cisco.com, which includes the Cisco Technical Assistance Center (TAC) website, as a starting point for all technical assistance. Customers and partners can obtain online documentation, troubleshooting tips, and sample configurations from the Cisco TAC website. Cisco.com registered users have complete access to the technical support resources on the Cisco TAC website, including TAC tools and utilities.

Cisco.com

Cisco.com offers a suite of interactive, networked services that let you access Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world.

Cisco.com provides a broad range of features and services to help you with these tasks:

- Streamline business processes and improve productivity
- Resolve technical issues with online support
- Download and test software packages
- Order Cisco learning materials and merchandise
- Register for online skill assessment, training, and certification programs

To obtain customized information and service, you can self-register on Cisco.com at this URL:

http://tools.cisco.com/RPF/register/register.do

RQS Nº 03/2005 - CN
CPMI - CORREIOS
21
0475
Fls:
3701
Doc:

Technical Assistance Center

The Cisco TAC is available to all customers who need technical assistance with a Cisco product, technology, or solution. Two types of support are available: the Cisco TAC website and the Cisco TAC Escalation Center. The type of support that you choose depends on the priority of the problem and the conditions stated in service contracts, when applicable.

We categorize Cisco TAC inquiries according to urgency:

- Priority level 4 (P4)—You need information or assistance concerning Cisco product capabilities, product installation, or basic product configuration. There is little or no impact to your business operations.
- Priority level 3 (P3)—Operational performance of the network is impaired, but most business operations remain functional. You and Cisco are willing to commit resources during normal business hours to restore service to satisfactory levels.
- Priority level 2 (P2)—Operation of an existing network is severely degraded, or significant aspects of your business operations are negatively impacted by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.
- Priority level 1 (P1)—An existing network is "down," or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Cisco TAC Website

The Cisco TAC website provides online documents and tools to help troubleshoot and resolve technical issues with Cisco products and technologies. To access the Cisco TAC website, go to this URL:

http://www.cisco.com/tac

All customers, partners, and resellers who have a valid Cisco service contract have complete access to the technical support resources on the Cisco TAC website. Some services on the Cisco TAC website require a Cisco.com login ID and password. If you have a valid service contract but do not have a login ID or password, go to this URL to register:

http://tools.cisco.com/RPF/register/register.do

If you are a Cisco.com registered user, and you cannot resolve your technical issues by using the Cisco TAC website, you can open a case online at this URL:

http://www.cisco.com/tac/caseopen

If you have Internet access, we recommend that you open P3 and P4 cases online so that you can fully describe the situation and attach any necessary files.

Cisco TAC Escalation Center

The Cisco TAC Escalation Center addresses priority level 1 or priority level 2 issues. These classifications are assigned when severe network degradation significantly impacts business operations. When you contact the TAC Escalation Center with a P1 or P2 problem, a Cisco TAC engineer automatically opens a case.

To obtain a directory of toll-free Cisco TAC telephone numbers for your country, go to this URL:

http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml

Before calling, please check with your network operations center to determine the Cisco support services to which your company is entitled: for example, SMARTnet, SMARTnet Onsite, or Network Supported Accounts (NSA). When you call the center, please have available your service agreement number and your product serial number.

11 Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- The *Cisco Product Catalog* describes the networking products offered by Cisco Systems, as well as ordering and customer support services. Access the *Cisco Product Catalog* at this URL:

  http://www.cisco.com/en/US/products/products_catalog_links_launch.html

- Cisco Press publishes a wide range of networking publications. Cisco suggests these titles for new and experienced users: *Internetworking Terms and Acronyms Dictionary, Internetworking Technology Handbook, Internetworking Troubleshooting Guide,* and the *Internetworking Design Guide.* For current Cisco Press titles and other information, go to Cisco Press online at this URL:

  http://www.ciscopress.com

- *Packet* magazine is the Cisco quarterly publication that provides the latest networking trends, technology breakthroughs, and Cisco products and solutions to help industry professionals get the most from their networking investment. Included are networking deployment and troubleshooting tips, configuration examples, customer case studies, tutorials and training, certification information, and links to numerous in-depth online resources. You can access *Packet* magazine at this URL:

  http://www.cisco.com/go/packet

- iQ Magazine is the Cisco bimonthly publication that delivers the latest information about Internet business strategies for executives. You can access iQ Magazine at this URL:

  http://www.cisco.com/go/iqmagazine

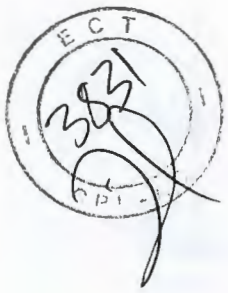
- Internet Protocol Journal is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

  http://www.cisco.com/en/US/about/ac123/ac147/about_cisco_the_internet_protocol_journal.html

- Training—Cisco offers world-class networking training. Current offerings in network training are listed at this URL:

  http://www.cisco.com/en/US/learning/le31/learning_recommended_training_list.html

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0476
Fls:
Doc: 3701



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. 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

Copyright © 2003 Cisco Systems, Inc. All rights reserved. CCIP, CCSP, the Cisco Arrow logo, the Cisco *Powered* Network mark, Cisco Unity, Follow Me Browsing, FormShare, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherSwitch, Fast Step, GigaStack, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, MGX, MICA, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, RateMUX, Registrar, ScriptShare, SlideCast, SMARTnet, StrataView Plus, Stratm, SwitchProbe, TeleRouter, The Fastest Way to Increase Your Internet Quotient, TransPath, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0304R)

Printed in the USA on recycled paper containing 10% postconsumer waste.

78-13503-04

DOC-7813503=

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0477
Fls:
3701
Doc:

CHAPTER 12

Administrators and Administrative Policy

This chapter addresses the Cisco Secure Access Control Server (Cisco Secure ACS) Appliance version 3.2 features found in the Administration Control section of the HTML interface. It contains the following sections:

- Administrator Accounts, page 12-1
- Access Policy, page 12-11
- Session Policy, page 12-16

Administrator Accounts

This section provides details about Cisco Secure ACS administrators. It contains the following topics:

- About Administrator Accounts, page 12-2
- Administrator Privileges, page 12-2
- Adding an Administrator Account, page 12-6
- Editing an Administrator Account, page 12-8
- Unlocking a Locked Out Administrator Account, page 12-10
- Deleting an Administrator Account, page 12-11

About Administrator Accounts

Administrators are the only users of the Cisco Secure ACS HTML interface. To access the Cisco Secure ACS HTML interface from a browser, you must log in to Cisco Secure ACS using an administrator account.

Note Cisco Secure ACS administrator accounts are unique to Cisco Secure ACS. They are not related to administrator accounts for your network, operating systems, or other software.

In the HTML interface, an administrator can configure any of the features provided in Cisco Secure ACS; however, the ability to access various parts of the HTML interface can be limited by revoking privileges to those parts of the HTML interface that a given administrator is not permitted to access.

For example, you may want to limit access to the Network Configuration section of the HTML interface to the administrators whose responsibilities include network management. To do so, you would select only the Network Configuration privilege for the applicable administrator accounts. For more information about administrator privileges, see Administrator Privileges, page 12-2.

Cisco Secure ACS administrator accounts have no correlation with Cisco Secure ACS user accounts or network user authentication. Cisco Secure ACS stores accounts created for authentication of network service requests and those created for Cisco Secure ACS administrative access in separate internal databases.

Administrator Privileges

You can grant appropriate privileges to each Cisco Secure ACS administrator by assigning privileges on an administrator-by-administrator basis. You control privileges by selecting the options in the Administrator Privileges table on the Add Administrator or Edit Administrator pages. These options are listed below:

- **User and Group Setup**—Contains the following privilege options for the User Setup and Group Setup sections of the HTML interface:
  - **Add/Edit users in these groups**—Enables the administrator to add or edit users and to assign users to groups in the Editable groups list.

- **Setup of these groups**—Enables the administrator to edit the settings for the groups in the Editable groups list.
- **Available Groups**—Lists the user groups for which the administrator *does not* have edit privileges and to which the administrator *cannot* add users.
- **Editable Groups**—Lists the user groups for which the administrator *does* have edit privileges and to which the administrator account *can* add users.

- **Shared Profile Components**—Contains the following privilege options for the Shared Profile Components section of the HTML interface:
  - **Network Access Restriction Sets**—Allows the administrator full access to the Network Access Restriction Sets feature.
  - **Downloadable ACLs**—Allows the administrator full access to the Downloadable PIX ACLs feature.
  - **Create New Device Command Set Type**—Allows the administrator account to be used as valid credentials by another Cisco application for adding new device command set types. New device command set types that are added to Cisco Secure ACS using this privilege appear in the Shared Profile Components section of the HTML interface.
  - **Shell Command Authorization Sets**—Allows the administrator full access to the Shell Command Authorization Sets feature.
  - **PIX Command Authorization Sets**—Allows the administrator full access to the PIX Command Authorization Sets feature.

Note Additional command authorization set privilege options may appear, if other Cisco network management applications, such as CiscoWorks2000, have updated the configuration of Cisco Secure ACS.

- **Network Configuration**—Allows the administrator full access to the features in the Network Configuration section of the HTML interface.

CPMI - CORREIOS
0479
Fls: 3701
Doc:

- **System Configuration...**—Contains the privilege options for the features found in the System Configuration section of the HTML interface. For each of the following features, enabling the option allows the administrator full access to the feature.
  - **Service Control**—For more information about this feature, see Service Control, page 8-2.
  - **Date/Time Format Control**—For more information about this feature, see Date Format Control, page 8-3.
  - **Logging Control**—For more information about this feature, see Logging, page 8-3.
  - **Local Password Management**—For more information about this feature, see Local Password Management, page 8-5.
  - **DB Replication**—For more information about this feature, see CiscoSecure Database Replication, page 9-1.
  - **RDBMS Synchronization**—For more information about this feature, see RDBMS Synchronization, page 9-23.
  - **IP Pool Address Recovery**—For more information about this feature, see IP Pools Address Recovery, page 9-44.
  - **IP Pool Server Configuration**—For more information about this feature, see IP Pools Server, page 9-37.
  - **ACS Backup**—For more information about this feature, see Cisco Secure ACS Backup, page 8-8.
  - **ACS Restore**—For more information about this feature, see Cisco Secure ACS System Restore, page 8-13.
  - **ACS Service Management**—For more information about this feature, see Cisco Secure ACS Active Service Management, page 8-17.
  - **VoIP Accounting Configuration**—For more information about this feature, see VoIP Accounting Configuration, page 8-21.
  - **ACS Certificate Setup**—For more information about this feature, see Cisco Secure ACS Certificate Setup, page 10-15.
  - **Global Authentication Setup**—For more information about this feature, see Global Authentication Setup, page 10-11.
  - **Appliance Configuration**—For more information about this feature, see Appliance Configuration, page 8-22.

ECT 3816 CPI-AC

  - **Support Operations**—For more information about this feature, see Support, page 8-24.
  - **View Diagnostic Logs**—For more information about this feature, see Viewing or Downloading Diagnostic Logs, page 8-27.
  - **Appliance Upgrade Status**—For more information about this feature, see Viewing or Downloading Diagnostic Logs, page 8-27.
- **Interface Configuration**—Allows the administrator full access to the features in the Interface Configuration section of the HTML interface.
- **Administration Control**—Allows the administrator full access to the features in the Administration Control section of the HTML interface.
- **External User Databases**—Allows the administrator full access to the features in the External User Databases section of the HTML interface.
- **Reports & Activity**—Contains the privilege options for the reports and features found in the Reports and Activity section of the HTML interface. For each of the following features, enabling the option allows the administrator full access to the feature.
  - **TACACS+ Accounting**—For more information about this report, see Accounting Logs, page 11-5.
  - **TACACS+ Administration**—For more information about this report, see Accounting Logs, page 11-5.
  - **RADIUS Accounting**—For more information about this report, see Accounting Logs, page 11-5.
  - **VoIP Accounting**—For more information about this report, see Accounting Logs, page 11-5.
  - **Passed Authentications**—For more information about this report, see Accounting Logs, page 11-5.
  - **Failed Attempts**—For more information about this report, see Accounting Logs, page 11-5.
  - **Logged-in Users**—For more information about this report, see Accounting Logs, page 11-5.
  - **Purge of Logged-in Users**—For more information about this feature, see Deleting Logged-in Users, page 11-9.
  - **Disabled Accounts**—For more information about this report, see Deleting Logged-in Users, page 11-9.

RQS Nº 03/2005 - CN - CPMI - CORREIOS
12-5
0480
Fls: 3701
Doc:

- **ACS Backup and Restore**—For more information about this report, see Deleting Logged-in Users, page 11-9.
- **DB Replication**—For more information about this report, see Deleting Logged-in Users, page 11-9.
- **RDBMS Synchronization**—For more information about this report, see Deleting Logged-in Users, page 11-9.
- **Administration Audit**—For more information about this report, see Deleting Logged-in Users, page 11-9.
- **ACS Service Monitor**—For more information about this report, see Deleting Logged-in Users, page 11-9.
- **User Change Password**—For more information about this report, see Deleting Logged-in Users, page 11-9.
- **Appliance Status**—For more information about this report, see Deleting Logged-in Users, page 11-9.
- **Appliance Administration Audit**—For more information about this report, see Deleting Logged-in Users, page 11-9.

Adding an Administrator Account

Before You Begin

For descriptions of the options available while adding an administrator account, see Administrator Privileges, page 12-2.

To add a Cisco Secure ACS administrator account, follow these steps:

Step 1 In the navigation bar, click **Administration Control**.

Step 2 Click **Add Administrator**.

Result: The Add Administrator page appears.

Step 3 Complete the boxes in the Administrator Details table:

a. In the Administrator Name box, type the login name (up to 32 characters) for the new Cisco Secure ACS administrator account.

b. In the Password box, type the password (up to 32 characters) for the new Cisco Secure ACS administrator account.

c. In the Confirm Password box, type the password a second time.

Step 4 To select all privileges, including user group editing privileges for all user groups, click **Grant All**.

Result: All privilege options are selected. All user groups move to the Editable groups list.

Tip To clear all privileges, including user group editing privileges for all user groups, click **Revoke All**.

Step 5 To grant user and user group editing privileges, follow these steps:

a. Select the desired check boxes under User & Group Setup.

b. To move a user group to the Editable groups list, select the group in the Available groups list, and then click —> (right arrow button).

Result: The selected group moves to the Editable groups list.

c. To remove a user group from the Editable groups list, select the group in the Editable groups list, and then click <— (left arrow button).

Result: The selected group moves to the Available groups list.

d. To move all user groups to the Editable groups list, click >>.

Result: The user groups in the Available groups list move to the Editable groups list.

e. To remove all user groups from the Editable groups list, click <<.

Result: The user groups in the Editable groups list move to the Available groups list.

Step 6 To grant any of the remaining privilege options, in the Administrator Privileges table, select the applicable check boxes.

Step 7 Click **Submit**.

Result: Cisco Secure ACS saves the new administrator account. The new account appears in the list of administrator accounts on the Administration Control page.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
12-7
Fls: 0481
Doc: 3701

Editing an Administrator Account

You can edit a Cisco Secure ACS administrator account to change the privileges granted to the administrator. You can effectively disable an administrator account by revoking all privileges.

Note You cannot change the name of an administrator account; however, you can delete an administrator account and then create an account with the new name. For information about deleting an administrator account, see Deleting an Administrator Account, page 12-11. For information about creating an administrator account, see Adding an Administrator Account, page 12-6.

For information about administrator privilege options, see Administrator Privileges, page 12-2.

Before You Begin

For descriptions of the options available while editing an administrator account, see Administrator Privileges, page 12-2.

To edit Cisco Secure ACS administrator account privileges, follow these steps:

Step 1 In the navigation bar, click **Administration Control**.

Result: Cisco Secure ACS displays the Administration Control page.

Step 2 Click the name of the administrator account whose privileges you want to edit.

Result: The Edit Administrator *name* page appears, where *name* is the name of the administrator account you just selected.

Step 3 To change the administrator password, follow these steps:

a. In the Password box, double-click the asterisks, and then type the new password (up to 32 characters) for the administrator.

Result: The new password replaces the existing, masked password.

b. In the Confirm Password box, double-click the asterisks, and then type the new administrator password a second time.

Result: The new password is effective immediately after you click Submit in Step 9.

Step 4 If the Reset current failed attempts count check box appears below the Confirm Password box and you want to allow the administrator whose account you are editing to access the Cisco Secure ACS HTML interface, select the **Reset current failed attempts count** check box.

Note If the Reset current failed attempts count check box appears below the Confirm Password box, the administrator cannot access Cisco Secure ACS unless you complete Step 4. For more information about re-enabling an administrator account, see Unlocking a Locked Out Administrator Account, page 12-10.

Step 5 To select all privileges, including user group editing privileges for all user groups, click **Grant All**.

Result: All privilege options are selected. All user groups move to the Editable groups list.

Step 6 To clear all privileges, including user group editing privileges for all user groups, click **Revoke All**.

Result: All privileges options are cleared. All user groups move to the Available groups list.

Step 7 To grant user and user group editing privileges, follow these steps:

a. Under User & Group Setup, select the applicable check boxes.

b. To move all user groups to the Editable groups list, click >>.

Result: The user groups in the Available groups list move to the Editable groups list.

c. To move a user group to the Editable groups list, select the group in the Available groups list, and then click —> (right arrow button).

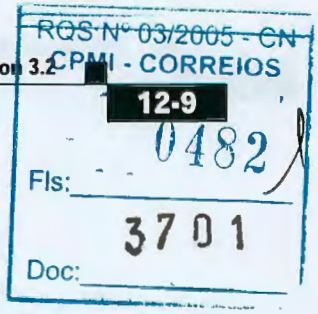
Result: The selected group moves to the Editable groups list.

d. To remove all user groups from the Editable groups list, click <<.

Result: The user groups in the Editable groups list move to the Available groups list.

e. To remove a user group from the Editable groups list, select the group in the Editable groups list, and then click <— (left arrow button).

Result: The selected group moves to the Available groups list.



Step 8 To grant any remaining privilege options, select the applicable check boxes in the Administrator Privileges table.

Step 9 To revoke any remaining privilege options, clear the applicable check boxes in the Administrator Privileges table.

Step 10 Click **Submit**.

Result: Cisco Secure ACS saves the changes to the administrator account.

Unlocking a Locked Out Administrator Account

Cisco Secure ACS disables the accounts of administrators who have attempted to access the Cisco Secure ACS HTML interface and have provided an incorrect password in more successive attempts than is specified on the Session Policy Setup page. Until the failed attempts counter for a disabled administrator account is reset, the administrator cannot access the HTML interface.

For more information about configuring how many successive failed login attempts can occur before Cisco Secure ACS disables an administrator account, see Session Policy, page 12-16.

To reset the failed attempts count for an administrator, follow these steps:

Step 1 In the navigation bar, click **Administration Control**.

Result: Cisco Secure ACS displays the Administration Control page.

Step 2 Click the name of the administrator account whose account you want to re-enable.

Result: The Edit Administrator *name* page appears, where *name* is the name of the administrator account you just selected.

If the Reset current failed attempts count check box appears below the Confirm Password box, the administrator account cannot access the HTML interface.

Step 3 Select the **Reset current failed attempts count** check box.

Step 4 Click **Submit**.

Result: Cisco Secure ACS saves the changes to the administrator account.

Deleting an Administrator Account

You can delete a Cisco Secure ACS administrator account when you no longer need it. We recommend deleting any unused administrator accounts.

To delete a Cisco Secure ACS administrator account, follow these steps:

Step 1 In the navigation bar, click **Administration Control**.

Result: Cisco Secure ACS displays the Administration Control page.

Step 2 In the Administrators table, click the name of the administrator account that you want to delete.

Result: The Edit Administrator *name* page appears, where *name* is the name of the administrator account you just selected.

Step 3 Click **Delete**.

Result: Cisco Secure ACS displays a confirmation dialog box.

Step 4 Click **OK**.

Result: Cisco Secure ACS deletes the administrator account. The Administrators table on the Administration Control page no longer lists the administrator account that you deleted.

Access Policy

The Access Policy feature affects access to the Cisco Secure ACS HTML interface. You can limit access by IP address and by the TCP port range used for administrative sessions. You can also enable secure socket layer (SSL) for access to the HTML interface.

This section contains the following topics:

- Access Policy Options, page 12-12
- Setting Up Session Policy, page 12-16

RQS Nº 03/2005 - CN - CPMI - CORREIOS
12-11
0483
Fls:
3701
Doc:

Access Policy Options

You can configure the following options on the Access Policy Setup page:

- **IP Address Filtering**—Contains the following IP address filtering options:
  - **Allow all IP addresses to connect**—Allow access to the HTML interface from any IP address.
  - **Allow only listed IP addresses to connect**—Allow access to the HTML interface only from IP addresses *inside* the address range(s) specified in the IP Address Ranges table.
  - **Reject connections from listed IP addresses**—Allow access to the HTML interface only from IP addresses *outside* the address range(s) specified in the IP Address Ranges table.
- **IP Address Ranges**—The IP Address Ranges table contains ten rows for configuring IP address ranges. The ranges are always inclusive; that is, the range includes the start and end IP addresses. The IP addresses entered to define a range must differ only in the last octet (Class C format).

  The IP Address Ranges table contains one column of each of the following boxes:
  - **Start IP Address**—Defines the lowest IP address of the range specified in the current row.
  - **End IP Address**—Defines the highest IP address of the range specified in the current row.
- **HTTP Port Allocation**—Contains the following options for configuring TCP ports used for remote access to the HTML interface.
  - **Allow any TCP ports to be used for Administration HTTP Access**—Allow the ports used by administrative HTTP sessions to include the full range of TCP ports.
  - **Restrict Administration Sessions to the following port range From Port *X* to Port *Y***—Restrict the ports used by administrative HTTP sessions to the range specified in the *X* and *Y* boxes, inclusive. The size of the range specified determines the maximum number of concurrent administrative sessions.

Cisco Secure ACS uses port 2002 to start all administrative sessions. You do not need to include port 2002 in the port range. Also, Cisco Secure ACS does not allow you to define an HTTP port range that consists only of port 2002. Your port range must consist of at least one port other than port 2002.

A firewall configured to permit HTTP traffic over the Cisco Secure ACS administrative port range must also permit HTTP traffic through port 2002, because this is the port a web browser must address to initiate an administrative session.

Note We do not recommend allowing administration of Cisco Secure ACS from outside a firewall. If you do choose to allow access to the HTML interface from outside a firewall, keep the HTTP port range as narrow as possible. This can help prevent accidental discovery of an active administrative port by unauthorized users. An unauthorized user would have to impersonate, or "spoof," the IP address of a legitimate host to make use of the active administrative session HTTP port.

- **Secure Socket Layer Setup**—The Use HTTPS Transport for Administration Access check box defines whether Cisco Secure ACS uses secure socket layer protocol to encrypt HTTP traffic between the CSAdmin service and a web browser used to access the HTML interface. When this option is enabled, all HTTP traffic between the browser and Cisco Secure ACS is encrypted, as reflected by the URLs, which begin with HTTPS. Additionally, most browsers include an indicator for when a connection is SSL-encrypted.

  To enable SSL, you must have completed the steps in Installing a Cisco Secure ACS Certificate, page 10-15 and Adding a Certificate Authority Certificate, page 10-18.

Setting Up Access Policy

For information about access policy options, see Access Policy Options, page 12-12.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
12-13
0484
Fls:
Doc: 3701

Before You Begin

If you want to enable SSL for administrative access, before completing this procedure, you must have completed the steps in Installing a Cisco Secure ACS Certificate, page 10-15 and Adding a Certificate Authority Certificate, page 10-18.

To set up Cisco Secure ACS Access Policy, follow these steps:

Step 1 In the navigation bar, click **Administration Control**.

Result: Cisco Secure ACS displays the Administration Control page.

Step 2 Click **Access Policy**.

Result: The Access Policy Setup page appears.

Step 3 To allow remote access to the HTML interface from any IP address, in the IP Address Filtering table, select the **Allow all IP addresses to connect** option.

Step 4 To allow remote access to the HTML interface only from IP addresses *within* a range or ranges of IP addresses, follow these steps:

a. In the IP Address Filtering table, select the **Allow only listed IP addresses to connect** option.

b. For each IP address range from within which you want to allow remote access to the HTML interface, complete one row of the IP Address Ranges table. In the Start IP Address box, type the lowest IP address (up to 16 characters) in the range. In the End IP Address box, type the highest IP address (up to 16 characters) in the range. Use dotted decimal format.

Note The IP addresses entered to define a range must differ only in the last octet.

Step 5 To allow remote access to the HTML interface only from IP addresses *outside* a range or ranges of IP addresses, follow these steps:

a. In the IP Address Filtering table, select the **Reject connections from listed IP addresses** option.

b. For each IP address range from outside which you want to allow remote access to the HTML interface, complete one row of the IP Address Ranges table. Type the lowest IP address (up to 16 characters) in the range in the Start IP Address box. Type the highest IP address (up to 16 characters) in the range in the End IP Address box.

Note The IP addresses entered to define a range must differ only in the last octet.

Step 6 If you want to allow Cisco Secure ACS to use any valid TCP port for administrative sessions, under HTTP Port Allocation, select the **Allow any TCP ports to be used for Administration HTTP Access** option.

Step 7 If you want to allow Cisco Secure ACS to use only a specified range of TCP ports for administrative sessions, follow these steps:

a. Under HTTP Port Allocation, select the **Restrict Administration Sessions to the following port range From Port *X* to Port *Y*** option.

b. In the *X* box type the lowest TCP port (up to 5 characters) in the range.

c. In the *Y* box type the highest TCP port (up to 5 characters) in the range.

Step 8 If you want to enable SSL encryption of administrator access to the HTML interface, under Secure Socket Layer Setup, select the **Use HTTPS Transport for Administration Access** check box.

Note To enable SSL, you must have completed the steps in Installing a Cisco Secure ACS Certificate, page 10-15 and Adding a Certificate Authority Certificate, page 10-18.

Step 9 Click **Submit**.

Result: Cisco Secure ACS saves and begins enforcing the access policy settings.

If you have enabled SSL, at the next administrator login, Cisco Secure ACS begins using HTTPS. Any current administrator sessions are unaffected.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
12-15
0485
Fls:
3701
Doc:

Session Policy

The Session Policy feature controls various aspects of Cisco Secure ACS administrative sessions. This section contains the following topics:

- Session Policy Options, page 12-16
- Setting Up Session Policy, page 12-16

Session Policy Options

You can configure the following options on the Session Policy Setup page:

- **Session idle timeout (minutes)**—Defines the time in minutes that an administrative session must remain idle before Cisco Secure ACS terminates the connection. This parameter applies to the Cisco Secure ACS administrative session in the browser only. It does not apply to an administrator dial-up session.

  An administrator whose administrative session is terminated receives a dialog box asking whether or not the administrator wants to continue. If the administrator chooses to continue, Cisco Secure ACS starts a new administrative session.

- **Respond to Invalid IP Address Connections**—Enables an error message in response to attempts to start a remote administrative session using an IP address that is invalid according to the IP address ranges configured in Access Policy. Disabling this option can help prevent unauthorized users from discovering Cisco Secure ACS.

- **Lock out Administrator after *X* successive failed attempts** —Enables Cisco Secure ACS to lock out an administrator after the number of successive failed login attempts specified in the *X* box. A value of 0 (zero) in the X box allows unlimited successive administrative login failures. If this check box is selected, the X box cannot be set to zero.

Setting Up Session Policy

For information about session policy options, see Session Policy Options, page 12-16.

To setup Cisco Secure ACS Session Policy, follow these steps:

Step 1 In the navigation bar, click **Administration Control**.

Result: Cisco Secure ACS displays the Administration Control page.

Step 2 Click **Session Policy**.

Result: The Session Policy Setup page appears.

Step 3 To define the number of minutes of inactivity after which Cisco Secure ACS ends an administrative session, in the Session idle timeout (minutes) box, type the number of minutes (up to 4 characters).

Step 4 Set the invalid IP address response policy:

a. To configure Cisco Secure ACS to respond with a message when an administrative session is requested from an invalid IP address, select the **Respond to invalid IP address connections** check box.

b. To configure Cisco Secure ACS to send no message when an administrative session is requested from an invalid IP address, clear the **Respond to invalid IP address connections** check box.

Step 5 Set the failed administrative login attempts policy:

a. To enable Cisco Secure ACS to lock out an administrator after a number of successive failed administrative login attempts, select the **Lock out Administrator after *X* successive failed attempts** check box.

b. In the *X* box, type the number of successive failed login attempts after which Cisco Secure ACS locks out an administrator. The *X* box accepts up to 4 characters.

Step 6 Click **Submit**.

Result: Cisco Secure ACS saves and begins enforcing the session policy settings you made.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
12-17
0486
Fls:
3701
Doc:

JP BC

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 0487
Doc: 3701

C T
3812
C P I A

Cisco Systems

Data Sheet

Cisco Secure **Access Control Server** Solution Engine

The Cisco® Secure Access Control Server (ACS) provides a comprehensive identity networking solution and secure user experience for Cisco intelligent information networks. It is the integration and control layer among all enterprise users, administrators, and the resources of the network infrastructure. The Cisco Secure ACS Solution Engine adds new security improvements, simplified management, and reduced total cost of ownership (TCO) for the operation of the underlying ACS service.

Introduction

The Cisco Secure ACS Solution Engine is a high-performance and highly scalable user and administrative access control solution that operates as a centralized RADIUS or TACACS+ server system for the Cisco 1111 platform. Packaged in a dedicated and secure 1-rack-unit (1-RU) hardened appliance, the Cisco Secure ACS Solution Engine provides a reduced-configuration, plug and play solution, and highly reliable platform with the unique ability to protect existing networking infrastructure through fully Web-based remote-access and configuration capabilities.

The need for security appliances is rapidly increasing in today's IT space. Security, convenience, and ease of installation and troubleshooting are the important advantages of security appliances compared to the many software-based security applications that exist in the marketplace today. The innovative, new, 1-RU, security-hardened Cisco Secure ACS Solution Engine was designed to specifically alleviate the security issue with a closed-device design that makes it substantially more difficult for intruders to penetrate than an open-platform system.

Security appliances provide an all-in-one approach that simplifies product selection, product integration, and ongoing support. By combining all necessary operating system installation and patching with the ACS software service, customers can avoid maintaining software versioning and proliferation of servers, patches, and operating system (OS) maintenance issues. This is particularly important in large networking environments where security solutions are required in remote sites with no IT professionals present to regularly manage and upgrade these solutions. In addition, a security appliance greatly simplifies support and troubleshooting in failure modes, hence enabling quick service restoration (through a one-stop support contact)—an important consideration, especially when the security application is mission-critical, a situation that is true with security authentication, authorization, and accounting (AAA) applications.

Changing network dynamics and increased security threats have influenced new opportunities in access control management solutions. As AAA becomes more relevant and the requirement to

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 0488
Doc: 3701

Cisco Systems, Inc.
All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

control user access expands beyond just dialup, new trends (including expanded authentication, tracking, and audit management) are emerging that require identity-networking solutions to be pervasive, scalable, and available throughout the network.

Cisco Secure ACS extends access security by combining authentication, user or administrator access, and policy control from a centralized location, allowing for greater flexibility and mobility, increased security, and user productivity gains. As an accounting service, the Cisco Secure ACS Solution Engine reduces IT operations costs by providing detailed reporting and monitoring capabilities of network users' behavior and by keeping a record of every access connection and device configuration change across the entire network.

Cisco Secure ACS provides a centralized identity networking solution and simplified user-management experience across all Cisco devices and security-management applications. Cisco Secure ACS ensures enforcement of assigned policies by allowing network administrators to control:

- Who can log in to the network
- What privileges each user has in the network
- What accounting information is recorded in terms of security audits or account billing
- What access and command controls are enabled for each configuration administrator

Like the Cisco Secure ACS for Windows, the Cisco Secure ACS Solution Engine supports a wide array of access connection types, including wired or wireless LAN, dialup, broadband, content, storage, voice over-IP (VoIP), firewall, and virtual private networks (VPNs).

Cisco Secure ACS Solution Engine Highlights

The Cisco Secure ACS Solution Engine is a highly secure, OS-independent, and dedicated platform that offers a highly manageable access control solution with an increasingly reduced setup and troubleshooting time. The Cisco Secure ACS Solution Engine provides Plug and Play deployment, a highly reliable AAA solution, and increased TCO protection through the high availability and simplified day-to-day operation and management of the Cisco Secure ACS service. It provides the same features and functions as the Cisco Secure ACS for Windows, in a dedicated, security-hardened, application-specific appliance package. Customers with existing Windows-based Cisco Secure ACS deployments can add or upgrade to Cisco Secure ACS Solution Engines without any effect on existing AAA configurations, including remote logging and replication configurations. More information about the latest Cisco Secure ACS features is available from the Cisco Secure ACS for Windows data sheet.

To ensure the high-security posture of the Cisco Secure ACS Solution Engine, additional functions specific to operating and managing the Cisco Secure ACS Solution Engine are provided. Additionally, a Cisco Secure ACS remote agent is available with each Cisco Secure ACS Solution Engine to enable remote logging and Windows authentication. Forwarding all accounting data from the solution engine to a remote agent preserves disk space on the solution engine. It also improves AAA performance by eliminating the frequent and time-consuming disk writes required for local logging on the solution engine. Also, because a Cisco Secure ACS Solution Engine is never a member of a Microsoft Windows domain, the Cisco Secure ACS remote agent establishes the necessary Windows domain trust relationships for Windows-based authentication.

Table 1 lists additional functions provided by the Cisco Secure ACS Solution Engine. These functions are not available from the Cisco Secure ACS for Windows software product.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0489
Fls:
Doc: 3701

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Table 1 Functions Provided by the Cisco Secure ACS Solution Engine

Hardened underlying operating system	• The Cisco Secure ACS Solution Engine is dedicated to run only the Cisco Secure ACS service, thereby preventing any appliance-based OS changes, additions, or configuration modifications.
Serial console interface	• A serial console interface is provided on the Cisco Secure ACS Solution Engine for initial configuration, subsequent management of IP connections, access to the Cisco Secure ACS HTML interface, and application of upgrade and recovery procedures. • The serial console interface supports both serial line and Telnet connections through which the Cisco Secure ACS service can be reimaged, reloaded, and rebooted, both locally and remotely.
Solution Engine-specific management tools	• Integrated into the existing Cisco Secure ACS HTML interface, Solution Engine-specific management tools provide generic appliance-management capabilities, including backup, recovery, software upgrades, monitoring, maintenance, and troubleshooting functions. • The Cisco Secure ACS HTML interface is accessed though a secured Secure Sockets Layer (SSL)-based connection.
Cisco Secure ACS remote agent	• The Cisco Secure ACS remote agent provides two functions: authentication against Windows domains and remote logging capabilities of user accounting records. • Administrators can provision primary and backup Cisco Secure ACS remote agents in distributed Cisco Secure ACS configurations.
Port-based packet filtering	• The Cisco Secure ACS Solution Engine implements a packet-filtering service to block traffic on all but the necessary Cisco Secure ACS-specific TCP and UDP ports.
Network Timing Protocol (NTP) support	• The Cisco Secure ACS Solution Engine has built-in NTP functions to maintain network timing synchronization and consistency with other Cisco Secure ACS appliances or network devices.

Cisco Secure ACS Solution Engine-Specific Benefits

In addition to the many benefits the Cisco Secure ACS solution brings in controlling user and administrative AAA inside your network, the Cisco Secure ACS Solution Engine, with its 1-RU hardened form factor, adds specific security and operational advantages in the following areas:

- *Security*—With a security-hardened service focused on running exclusively the Cisco Secure ACS service, the solution engine significantly increases the security posture of the Cisco Secure ACS system. All solution engine services and ports not used by the Cisco Secure ACS service are disabled to secure access to the Cisco Secure ACS Solution Engine.
- *Plug and Play solution*—The Cisco Secure ACS Solution Engine provides a record service uptime before starting to configure the Cisco Secure ACS service.
- *Manageability*—With a dedicated, exclusive, and complete Cisco Secure ACS solution, the appliance greatly simplifies manageability and support of the Cisco Secure ACS service while removing the necessity to manage any UNIX or Windows network operating systems.
- *Supportability*—With no external services or applications (other than the Cisco Secure ACS service) allowed to be installed on the solution engine, the support and the day-to-day management of the Cisco Secure ACS Solution Engine are greatly simplified.

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

ECT 3810 CPL
RQS Nº 03/2005 - CN
CPMI - CORREIOS
0490
Fls:
3701
Doc:

- *Reliability*—Enabling only the services that are required by Cisco Secure ACS allows an increase in overall reliability and security of the Cisco Secure ACS service.
- *TCO*—With a turnkey security-hardened solution engine that is easily deployed, Cisco is able to guarantee full support, maintenance, and serviceability of the overall Cisco Secure ACS system—not just the Cisco Secure ACS software running on various hardware configurations, supported by third-party vendors.
- *Migration from Cisco Secure ACS UNIX*—The Cisco Secure ACS Solution Engine provides a suitable alternative for Cisco Secure ACS UNIX customers not willing to install or manage Cisco Secure ACS on the Windows OS.

System Requirements

Hardware Requirements

The Cisco Secure ACS Solution Engine is available on Cisco 1111 platforms with the following specifications:

- Pentium IV processor, 2.66 GHz
- 1 GB RAM
- 40 GB free disk space
- Two built-in 10/100 Ethernet controllers
- 1 floppy disk drive
- 1 CD-ROM drive

The Cisco Secure ACS remote agent is available in a Windows version that can be installed on a Windows 2000 Server (Windows Domain Controller or Member Server supported).

The computer running Cisco Secure ACS remote agent for Windows must meet the following minimum hardware requirements:

- Pentium III processor, 550 MHz or faster
- 256 MB RAM
- 250 MB free disk space

Ordering Information

The Cisco Secure ACS Solution Engine is available for purchase through normal Cisco sales and distribution channels worldwide. The Cisco Secure ACS Solution Engine is shipped with a preinstalled Cisco Secure ACS Software license.

For More Information

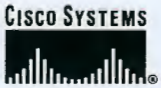
For more information about Cisco Secure ACS, visit: http://www.cisco.com/go/acs.

For specific product functions or technical questions, send e-mail to the Cisco Secure ACS product marketing group at ACS-MKT@cisco.com.

For questions about product ordering, availability, and support contract information, send e-mail to the product marketing group at ciscoworks@cisco.com.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0491
Fls: 3701
Doc:

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.



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

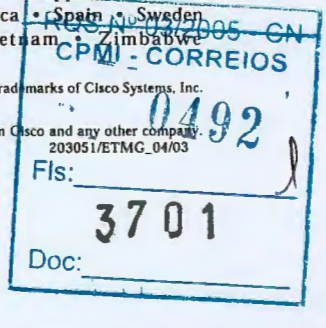
Cisco Web site at www.cisco.com/go/offices

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

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Cisco, Cisco Systems, the Cisco Systems logo, Aironet, Catalyst, and Cisco IOS are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0303R)

203051/ETMG_04/03



LP BD

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0493
Fls:
3901
Doc:

Cisco Systems

Q & A

Cisco Secure **Access Control Server** Solution Engine

Q. What is Cisco® Secure Access Control Server (ACS) Solution Engine?

A. Cisco Secure ACS Solution Engine is a highly scalable, one-rack-unit (RU), dedicated platform that serves as a high-performance access control server supporting centralized Remote Authentication Dial-In User Service (RADIUS) or Terminal Access Controller Access Control System (TACACS+). Cisco Secure ACS Solution Engine controls the authentication, authorization, and accounting (AAA) for users accessing corporate resources through the network.

Q. What does Cisco Secure ACS Solution Engine do?

A. Cisco Secure ACS Solution Engine enables you to control who can access the network, to authorize what types of network services are available for users or groups of users, and to keep an accounting record of all user actions in the network. The Solution Engine supports access control and accounting for dial-up access servers, firewalls and VPNs, voice-over-IP (VoIP) solutions, content networking, storage networks, and switched and wireless LANs (WLANs). In addition, the AAA framework can be used to manage the administrative roles and groups via TACACS+ and to control how network administrators are able to change, access, and configure the network internally.

Q. Why did Cisco add an Solution Engine to the existing Windows server software packaging for Cisco Secure ACS?

A. The decision to create a dedicated solution engine version of Cisco Secure ACS was made based on several factors:

- Security—The need to create a turnkey security-hardened service focused on running the Cisco Secure ACS service exclusively. The solution engine can remove all extraneous services, block all unused ports, and otherwise prevent all other access to the Cisco Secure ACS server system—dramatically increasing the security posture of Cisco Secure ACS.
- Manageability—Cisco Secure ACS Solution Engine is a dedicated, exclusive service for AAA with no ability to install or run other services or applications. This greatly facilitates the support and day-to-day management of the Cisco Secure ACS system.
- Reliability—By targeting only the operating system services required by Cisco Secure ACS, the solution engine offers greater operational reliability and security for the Cisco Secure ACS system.
- Total cost of ownership—Customers choosing Cisco Secure ACS can optimize their total cost of ownership. Cisco end-to-end support now includes

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 0494
Doc: 3701

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

full support, maintenance, and serviceability of the Cisco Secure ACS system—not just the Cisco Secure ACS software running on various hardware configurations and supported by various third-party vendors.

- Plug and play—Cisco Secure ACS Solution Engine is shipped already installed with Cisco Secure ACS application software, greatly reducing the time it takes to set up and deploy Cisco Secure ACS in your network.
- Migration from Cisco Secure ACS UNIX—Cisco Secure ACS Solution Engine was built and targeted as a suitable migration platform for Cisco Secure ACS for Unix customers not willing to install or manage Cisco Secure ACS on a Windows server.

Q. What are the differences between the Cisco Secure ACS software server and Cisco Secure ACS Solution Engine?

A. Cisco Secure ACS Solution Engine provides the same features and functions of the Cisco Secure ACS Windows version—in a dedicated, security-hardened, application-specific option. The appliance includes features specific to the operation and management of Cisco Secure ACS, and specific software features needed to be customized or removed due to the different underlying system architectures:

Authentication

- Authentication against a Windows domain requires a Cisco Secure ACS remote agent running on a domain controller or member server. The Cisco Secure ACS remote agent is necessary to establish a Windows member or domain controller trust relationship.
- Authentication against an Open Database Connectivity (ODBC) source is not supported. Lightweight Directory Access Protocol (LDAP) authentication can be used instead.
- Authentication against One-Time Password (OTP) directories is performed using the generic RADIUS-based OTP interface on the appliance. Any OTP vendor that provides an RFC-compliant RADIUS interface can interface with Cisco Secure ACS.

User Database Synchronization

- User database synchronization with an ODBC source is not supported. Instead, the administrator can configure Cisco Secure ACS to synchronize its user database with a comma-separated values (CSV) file on a remote File Transfer Protocol (FTP) server.

ODBC Logging

- ODBC logging is not supported. Administrators can use local or remote CSV logging.

Backup/Restore and Appliance Diagnostics

- Backup/restore and gathered appliance diagnostics are performed through a remote FTP server and configured using the current Cisco Secure ACS HTML graphical user interface (GUI).

Q. What additional features are available on Cisco Secure ACS Solution Engine but not available on the Windows version?

A. To ensure the highly secure posture of Cisco Secure ACS Solution Engine, functions specific to operating and managing the appliance have been added:

- Security-hardened underlying operating system.
- Port-based packet filtering, allowing connections only to the ports necessary for Cisco Secure ACS operation.
- Serial console interface for initial configuration, subsequent management of IP connections, Web interface, and application of upgrades and remote reboots. The serial console interface supports both serial line and Telnet connections.

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

- Backup/restore of Cisco Secure ACS data via FTP protocol.
- Recovery procedures.
- NTP (Network Time Protocol) support for maintaining network time consistency with other appliances or network devices.

Q. Are there any additions to the existing Cisco Secure ACS GUI to support Cisco Secure ACS Solution Engine?

A. Yes. New HTML pages specific to Cisco Secure ACS Solution Engine have been added to the Cisco Secure ACS GUI. These pages cover specific features around the operation and management of the solution engine and include:

- Solution Engine configuration page
- Solution Engine remote agent configuration page
- Solution Engine upgrade page
- Solution Engine status page
- Solution Engine diagnostics log view

Q. What ports and protocols access Cisco Secure ACS Solution Engine?

A. Cisco Secure ACS Solution Engine implements a packet filtering service to block the traffic on all but necessary TCP/User Datagram Protocol (UDP) ports. Only the ports listed in Table 1 are open for input traffic:

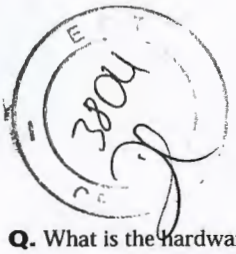
Table 1 Cisco Secure ACS Solution Engine Ports Usage

Service Name	UDP	TCP
DHCP	68	
RADIUS authentication and authorization (original draft RFC)	1645	
RADIUS accounting (original draft RFC)	1646	
RADIUS authentication and authorization (revised RFC)	1812	
RADIUS accounting (revised draft RFC)	1813	
TACACS+ AAA		49
Replication and RDBMS synchronization		2000
Cisco Secure ACS remote logging		2001
Cisco Secure ACS distributed logging (appliance only)		2003
Hypertext Transfer Protocol (HTTP) administrative access (at login)		2002
Administrative access (after login) port range		Configurable (default 1024-65535)[1]

1. ACS assigns unique port number from the range to each administration session

Cisco Systems, Inc.
All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 0495
Doc: 3701



Q. What is the hardware platform specification for Cisco Secure ACS Solution Engine?

A. Cisco Secure ACS Solution Engine is a security-hardened Cisco Secure ACS server in a dedicated 1-RU box with the following configuration:

- Intel ISP 1100 motherboard with a 2.66-GHz Pentium 4 processor
- 1 GB of RAM
- Two built-in 10/100 Ethernet controllers
- 40-GB IDE hard drive
- One floppy drive
- One CD-ROM drive

Q. How does Cisco Secure ACS Solution Engine authenticate to Windows domains?

A. In general, to authenticate Windows NT 4.0 or Active Directory domain users, you must establish a Windows member or domain controller trust relationship. Since Cisco Secure ACS Solution Engine does not run the necessary Windows server services to establish this trust, an external Cisco Secure ACS remote agent is provided with the appliance solution, allowing the trust relationship to be established. The Cisco Secure ACS remote agent can be installed on member servers, domain controllers, or backup domain controllers. NOTE: The best practice is to install the remote agent on a full Domain Controller (DC), as this would allow it to perform its authentication functions with the least extra configuration requirements.

Q. What is the main purpose of the Cisco Secure ACS remote agent?

A. The Cisco Secure ACS remote agent has dual roles—it enables authentication against Windows domains, and it allows remote logging capabilities of user accounting records.

Q. What operating systems can the Cisco Secure ACS remote agent be installed on?

A. The Cisco Secure ACS remote agent can be installed on a Windows 2000 server (Windows Domain Controller or Member Server supported). A Solaris version of Cisco Secure ACS will be provided in the future for Sun Solaris installations. Please refer to the Cisco Secure ACS remote agent installation guide for the exact operating system versions and service packs supported.

Q. Can a Cisco Secure ACS remote agent and Cisco Secure ACS Windows coexist on the same server?

A. No. The Cisco Secure ACS remote agent cannot be installed on a server that already has Cisco Secure ACS Windows installed.

Q. Can a solution engine be configured to use several remote agents?

A. Yes. A solution engine can be configured to use one or more agents. There is no restriction that the same agent be used for Windows services and logging services. For Windows services, an appliance can point to a primary and backup agent, in the event that the primary agent is unavailable.

Q. Can a Cisco Secure ACS remote agent be shared with multiple solution engines?

A. Yes. The Cisco Secure ACS remote agent can be shared with multiple solution engines. There is no hard limit to the number of Cisco Secure ACS solution engines that can share a single remote agent, but Cisco will support configurations with up to five solution engines sharing a single Cisco Secure ACS remote agent. If user accounting records from multiple Cisco Secure ACS solution engines need to be consolidated and centralized, it is desired that all these solution engines share a single Cisco Secure ACS remote agent.

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Q. Can I perform local logging on Cisco Secure ACS Solution Engine instead of using the remote logging capability of the Cisco Secure ACS remote agent?

A. Yes. However, local logging on Cisco Secure ACS Solution Engine is constrained in size, forcing log files to be recycled after seven days. The Cisco Secure ACS remote agent provides full, unconstrained logging capability to a remote server.

Q. Are there any differences in the type of Windows databases supported by the Cisco Secure ACS remote agent and the ones supported by Cisco Secure ACS Windows?

A. No. The Cisco Secure ACS remote agent supports the same Windows databases supported by Cisco Secure ACS Windows.

Q. What 802.1X authentication types does the Cisco Secure ACS remote agent support?

A. The Cisco Secure ACS remote agent supports the same 802.1X authentication types available on Cisco Secure ACS for Windows. This includes Extensible Authentication Protocol (EAP)-MD5, EAP-TLS, EAP Cisco Wireless, LEAP, PEAP-EAP-GTC, and PEAP-EAP-MSCHAPv2.

Q. Can a Cisco Secure ACS remote agent be provisioned for Cisco Secure ACS for Windows?

A. No. In its initial release, the Cisco Secure ACS remote agent only operates with Cisco Secure ACS Solution Engine. No communication is possible between a Cisco Secure ACS remote agent and a Cisco Secure ACS service on Windows. However, this limitation does not prevent Cisco Secure ACS Windows and Cisco Secure ACS Solution Engine from operating in the same network environment.

Q. What happens to the standard HTML reports on the solution engine? Do they stay the same?

A. In general, these reports stay the same. The solution engine reports will be constrained in size with no support for multiple rolled over files. The Cisco Secure ACS remote agent will provide full, unconstrained report capability on a remote FTP server.

Q. What happens with third-party software tools, such as backup services from Legato?

A. Cisco Secure ACS Solution Engine is a standalone, dedicated box for running Cisco Secure ACS. There are no interfaces or abilities to add third-party software of any kind to the box. Cisco will investigate third-party extensibility, but at present, nothing can be installed on the Cisco Secure ACS Solution Engine other than Cisco Secure ACS images and patches downloaded via FTP. For Cisco Secure ACS backup, Cisco will create an export file that is automatically exported to an external FTP server. Backup tools can be installed and used to backup the external server.

Q. Can I run Cisco Secure ACS in "mixed mode" (for example, run instances of the Cisco Secure ACS Windows and additional instances of Cisco Secure ACS Solution Engine)?

A. Yes. Cisco will support environments using both Cisco Secure ACS Windows and Cisco Secure ACS Solution Engine.

Q. How is Cisco Secure ACS replication affected with the introduction of Cisco Secure ACS Solution Engine?

A. Cisco Secure ACS replication functions will remain unchanged with the introduction of Cisco Secure ACS Solution Engine. Replication between Cisco Secure ACS Solution Engine and Cisco Secure ACS Windows, as well as replication among Cisco Secure ACS solution engines, will be supported with no impact on any of the solution engines or Windows configurations.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0496
Fls:
Doc: 3701

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Q. Are there any restrictions on whether Cisco Secure ACS Windows or Cisco Secure ACS Solution Engine can be a master database in a replicated configuration?

A. No. Cisco Secure ACS Windows or Cisco Secure ACS Solution Engine can be the master databases replicating to Cisco Secure ACS Windows slaves, Cisco Secure ACS Solution Engine slaves, or both Windows and solution engine slaves at the same time.

Q. Are there any changes to single logon and password aging capabilities in Cisco Secure ACS Solution Engine?

A. No. With the appropriate Windows or domain controller trust relationships established with the Cisco Secure ACS remote agent, single logon and password aging capabilities remain unchanged from Cisco Secure ACS Windows version.

Q. How scalable is a Cisco Secure ACS Solution Engine?

A. The Cisco Secure ACS Solution Engine follows, as a minimum, the same scalability performance as a Windows-based Cisco Secure ACS server. Cisco Secure ACS guidelines and performance analysis shows that each Cisco Secure ACS server can support anywhere from 20,000 to 80,000 users per server, and can scale to support in excess of 10,000 devices, depending on configuration, platform, and usage scenarios. The real challenge in scaling a user access control framework is on the back end. Linked to a high-performance back-end database such as Oracle or Sybase, Cisco has deployed Cisco Secure ACS for Windows 2000 and NT in clustered deployments into customers with hundreds of thousands of user records.

Q. What Cisco Secure ACS Solution Engine features enhance Cisco Secure ACS reliability and remote management?

A. The operating system is configured to automatically reboot on system crash. The serial console service is configured to automatically restart if it fails. Cisco Secure ACS software implements the monitor that will restart Cisco Secure ACS services if they fail. The solution engine also provides a remote administrator command line interface (CLI). The CLI supports both serial line and Telnet connections, and the Cisco Secure ACS service can be reimaged, reloaded, upgraded, and rebooted remotely from the CLI interface.

Q. What support is there for LDAP?

A. Support for LDAP on the appliance is identical to present support from the Cisco Secure ACS Software version. Cisco Secure ACS supports user authentication against records kept in a directory server through LDAP. Cisco Secure ACS supports the most popular directory servers, including Novell and Netscape LDAP Servers, through a generic LDAP interface.

Q. Will Cisco Secure ACS Solution Engine allow "single login" for Windows networking?

A. Yes. Cisco Secure ACS can be set up so that a user will only need to enter a user name and password once. This is considered a "single login." The Cisco Secure ACS remote agent is required to be installed on a Windows network server with the necessary trust relationships to the domain defined.

Q. Does Cisco Secure ACS support OTP and token systems?

A. Yes. Cisco Secure ACS can be configured to communicate with token solutions from ActiveCard, Cryptocard, PassGo Technologies, RSA Data Security, Secure Computing, and Vasco. Cisco Secure ACS Solution Engine includes a generic RADIUS interface for expanding OTP coverage to new vendors. Any OTP vendor that provides an RFC-compliant RADIUS interface should work with Cisco Secure ACS Solution Engine.

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Q. What's new in Cisco Secure ACS Version 3.2 for access control functions and features?

A. Cisco Secure ACS Version 3.2 is a minor update to Cisco Secure ACS Version 3.1. It adds the following main features:

- Cisco Secure ACS Solution Engine support
- EAP-MSCHAPv2 support within the Protected EAP (PEAP) framework (used for both wireless and wired environments)
- Machine-based authentication (through EAP-TLS and EAP-MSCHAPv2)
- PEAP authentication against the internal Cisco Secure ACS database
- EAP-TLS authentication against ODBC databases
- EAP-TLS session resume support
- Accounting support for Cisco Aironet® clients
- LDAP multithreading
- Downloadable access control lists (ACLs) for VPN solutions

Please refer to the Cisco Secure ACS Version 3.2 data sheet for more information about the features and functions introduced in this release.

Q. How is Cisco Secure ACS Solution Engine Version 3.2 licensed?

A. Cisco Secure ACS Solution Engine is licensed per server, with unlimited ports, users, and network access servers. The following solution engine packages will be available for ordering. For exact part numbers, refer to the Cisco Secure ACS Version 3.2 product bulletin at: http://www.cisco.com/go/acs

- Cisco Secure ACS Solution Engine Version 3.2
- Cisco Secure ACS Solution Engine upgrade package—Used for upgrading from software versions of Cisco Secure ACS 3.x or Cisco Secure ACS for UNIX to Cisco Secure ACS Solution Engine Version 3.2

Note: The Cisco Secure ACS Solution Engine upgrade package can be ordered when customers have deployed Cisco Secure ACS for Windows or Cisco Secure ACS for UNIX in their networks and want to upgrade to the solution engine version. Please refer to the Cisco Secure ACS Solution Engine user guide and release notes for supported upgrade paths. Current Cisco Secure ACS software maintenance entitlements do not provide a free upgrade to the Cisco Secure ACS Solution Engine.

Q. Can I upgrade to Cisco Secure ACS Version 3.2 from older software versions of Cisco Secure ACS?

A. Yes. A detailed upgrade procedure will be available to guide you through the required steps to complete an upgrade to Cisco Secure ACS Solution Engine. Please refer to the Cisco Secure ACS Solution Engine user guide for more information about the supported upgrade procedure.

Q. Can I purchase or license a backup solution engine?

A. No. An additional Cisco Secure ACS Solution Engine must be purchased as a separate Cisco Secure ACS server license to be used for recovery and backup purposes. Cisco Secure ACS servers can be run as recovery or failover servers. Because Cisco Secure ACS is a central control service in your network, Cisco highly recommends that customers configure a backup server for failover and recovery.

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 0497
Doc: 3701

Q. Does Cisco Secure ACS Solution Engine operating system need to be updated when upgrading the Cisco Secure ACS firmware?

A. No. Future Cisco Secure ACS image upgrades are applied to Cisco Secure ACS Solution Engine without updating or modifying the underlying Cisco Secure ACS Solution Engine operating system.

Q. Do I need to patch the solution engine with newer operating system releases or patches?

A. No. All operating system software updates and patches are handled by Cisco Secure ACS Solution Engine upgrades performed by Cisco. Any operating system patch that requires changes to Cisco Secure ACS Solution Engine will be provided in a new upgrade/patch.

Q. Can Cisco Secure ACS Solution Engine software be upgraded remotely from a CD-ROM?

A. Yes. Cisco Secure ACS Solution Engine supports remote upgrades from CD-ROM without any FTP server posting requirements.

Q. Can Cisco Secure ACS Solution Engine support software image rollback during patch update verification?

A. Yes. Cisco Secure ACS Solution Engine can roll back to previously installed software when a software patch has been applied. This capability is used for debugging and verification purposes.

Q. What is the status of Cisco Secure ACS for UNIX?

A. Cisco Secure ACS for UNIX is expected to be discontinued, at which point an end-of-life, end-of-sale (EOL/EOS) announcement will be made. Cisco will support all existing customers and provide smooth migration paths as the new platforms become available. The EOL/EOS date has not been determined, but Cisco will provide customer support for Cisco Secure ACS for UNIX customers for a period no shorter than 24 months after the EOL/EOS date. At present, no new features or releases are planned for Cisco Secure ACS for UNIX and only critical, Priority 1 bugs will be addressed.

Q. Can I use my current Cisco Secure ACS Windows maintenance contract to get support on Cisco Secure ACS Solution Engine?

A. No. Separate hardware and software contracts need to be purchased for maintenance support on Cisco Secure ACS Solution Engine. Please refer to refer to the Cisco Secure ACS Version 3.2 product bulletin for more information. http:// www.cisco.com/go/acs

Q. How can I obtain a demo of Cisco Secure ACS Solution Engine?

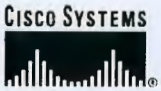
A. Please contact your Cisco account manager, who will be able to arrange for a limited time demo of Cisco Secure ACS Solution Engine.

Q. Where can I find more information on Cisco Secure ACS?

A. For additional product information, visit: http://www.cisco.com/go/acs

For additional information or questions, please send e-mail to the Cisco Secure ACS product marketing group at ACS-MKT@cisco.com.

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.



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

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Cisco, Cisco Systems, the Cisco Systems logo, and Aironet are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0303R)

203051/ETMG_05/03

Ap BE

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0499
Fls:
Doc: 3701

Supported and Interoperable Devices and Software Tables for Cisco Secure ACS Appliance version 3.2

Revised: July 8, 2003

Because the number of devices that Cisco Secure ACS Appliance version 3.2 interoperates with runs into the hundreds, this device list differs significantly from those of other Cisco products with which you may be familiar. This document lists supported devices and software, that is, those that we have tested against. However, this document also lists devices and software programs that are, to the best of our knowledge, interoperable. Of the hundreds of devices and software programs that Cisco Secure ACS Appliance version 3.2 interoperates with, Cisco officially supports only those that have been tested.

For details regarding other limitations and known problems see *Release Notes for CiscoSecure Access Control Server Appliance Version 3.2*. On Cisco.com, you can find the latest version all documentation by selecting **Products & Services > Security and VPN Software > Cisco Secure Access Control Server Appliance > Technical Documentation**.

CISCO SYSTEMS

Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Copyright © 2002. Cisco Systems, Inc. All rights reserved.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0500
Fls:
3701
Doc:

With regard to third-party RADIUS and TACACS+ clients, Cisco Secure ACS Appliance fully interoperates with devices that adhere to the governing protocols. Also, support for RADIUS and TACACS+ functions depends on device-specific implementation. On a given device, TACACS+ may not be available for user authentication and authorization. Likewise, RADIUS may not be available for administrative authentication and authorization.

For RADIUS these include the following RFCs:

- RFC 2138 - Remote Authentication Dial In User Service (RADIUS)
- RFC 2139 - RADIUS Accounting
- RFC 2865 - Remote Authentication Dial In User Service (RADIUS)
- RFC 2866 - RADIUS Accounting
- RFC 2867 - RADIUS Accounting for Tunnel Protocol Support
- RFC 2868 - RADIUS Attributes for Tunnel Protocol Support
- RFC 2869 - RADIUS Extensions

For details regarding the implementation of vendor-specific attributes (VSAs), see *User Guide for Cisco Secure ACS Appliance Version 3.2*.

Cisco Secure ACS Appliance conforms to the TACACS+ protocol as defined by Cisco Systems in draft 1.77.

The following tables show the devices and software that Cisco Secure ACS Appliance supports or with which it interoperates:

- Table 1, Web Browsers
- Table 2, Device Operating Systems
- Table 3, Routers
- Table 4, Access Devices/Universal Gateways
- Table 5, Cable Devices
- Table 6, Content Networking Devices
- Table 7, Security and VPN Devices
- Table 8, Storage Networking Devices
- Table 9, Switches
- Table 10, Cisco Aironet Software (Access Points for Wireless LAN)
- Table 11, CiscoWorks VMS

- Table 12, PKI/Certificate Servers
- Table 13, Token Servers
- Table 14, LDAP Servers
- Table 15, User Databases
- Table 16, Proxy Support

You can find information about new device support at Cisco.com, http://www.cisco.com.

To ensure full capabilities, the clients you deploy to interoperate with Cisco Secure ACS Appliance should use the most recent operating systems available. Nonetheless, Table 2 provides details on the minimum acceptable client operating system versions.

Table 1 Web Browsers[1]

Program	Versions	Notes
Microsoft Internet Explorer	5.5 for Microsoft Windows - English Language version	Tested
	6.0 for Microsoft Windows - English Language version	Tested
Netscape	7.0 for Microsoft Windows - English Language version	Tested
	7.0 on Solaris 2.7- English Language version	Tested

To use a web browser to access the Cisco Secure ACS HTML interface, you must enable both Java and JavaScript in the browser. Also, the web browser must not be configured to use a proxy server.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 3701
Doc:

Table 2 Device Operating Systems

Operating System	Minimum Version	Notes
IOS	11.2	For full RADIUS support
CAT OS	7.2	Cisco products—and other third-party products that are RFC compliant—will work with Cisco Secure ACS even when running earlier versions of CAT OS. However, full functionality, including the 802.1x VLAN assignment, is supported only when the listed version is used.

Table 3 Routers

Series	Notes
Cisco 1400	End of life (EOL) status
Cisco 1600	RADIUS and TACACS+ interoperability
Cisco 1700	Tested with IOS 12.2(8) RADIUS and TACACS+ interoperability
Cisco 2500	EOL status
Cisco 2600	RADIUS and TACACS+ interoperability
Cisco 3600	RADIUS and TACACS+ interoperability
Cisco 3700	Tested with IOS 12.2 RADIUS and TACACS+ interoperability
Cisco 7100	RADIUS and TACACS+ interoperability
Cisco 7200	Tested with IOS 12.2 RADIUS and TACACS+ interoperability
Cisco 7300	RADIUS and TACACS+ interoperability
Cisco7400	RADIUS and TACACS+ interoperability
Cisco 7500	RADIUS and TACACS+ interoperability

Table 3 Routers (continued)

Cisco 10000	RADIUS interoperability
Cisco 10720	RADIUS and TACACS+ interoperability

Table 4 Access Devices/Universal Gateways

Series	Notes
6400 Series	RADIUS and TACACS+ interoperability
5350 Series	RADIUS and TACACS+ interoperability
AS5400 Series	Tested with IOS12.2(7c) RADIUS and TACACS+ interoperability
AS5850 Series	RADIUS and TACACS+ interoperability
DSL Series / 6015, 6100, 6130, 6160, 6260	RADIUS and TACACS+ interoperability
MGX Series / 8220, 8250, 8800, 8950	TACACS+ interoperability

Table 5 Cable Devices

Devices	Notes
uBR7100	Tested with IOS 12.2BC RADIUS and TACACS+ interoperability
uBR7200	EOL status TACACS+ interoperability

Table 6 Content Networking Devices

Series / Devices	Notes
CE7300 / CE 7320	Tested with ACNS 4.2 RADIUS and TACACS+ interoperability

CPMI - [redacted] 03/2005 - CN
5
Fls: 0502
Doc:

Table 6 Content Networking Devices (continued)

Series / Devices	Notes
CDM4600 / CDM4630, CDM4650	RADIUS and TACACS+ interoperability
4400 Content Routers/ CR4430	Tested with ACNS 4.2 RADIUS and TACACS+ interoperability

Table 7 Security and VPN Devices

Series / Devices	Notes
3000 Series Concentrator / 3005, 3015, 3030, 3060, 3080	Tested with 3015 RADIUS and TACACS+ interoperability
PIX 500 Series Firewall / 501, 506E, 515, 515E, 525, 535	Tested with 515 and PIX OS v6.3 RADIUS and TACACS+ interoperability
5000 Series Concentrator	EOL status

Table 8 Storage Networking Devices

Series	Devices Supported	Notes
MDS 9000	MDS 9216, MDS9509	RADIUS interoperability (TACACS+ support in future release)

Table 9 Switches

Series / Devices	Notes
Catalyst 2950/3550	Tested with 3550 and IOS 12.1(12)EA1 RADIUS and TACACS+ interoperability
Catalyst 4000/4500	Tested with Cat4503, CatOS 7.5, and IOS 12.1 RADIUS and TACACS+ interoperability

Table 9 Switches (continued)

Series / Devices	Notes
Catalyst 5000	EOL status
Catalyst 6500	Tested with CatOS 7.5, and IOS 12.1 RADIUS and TACACS+ interoperability

Table 10 Cisco Aironet Software (Access Points for Wireless LAN)

ies	Notes
350	RADIUS interoperability
AP1100	RADIUS interoperability
AP1200	Tested with Aironet 11.23 RADIUS interoperability

Table 11 CiscoWorks VMS

Series	Devices Supported	Notes
IOS/Router MC	Version 1.1	TACACS+ interoperability
PIX MC	Version 1.1	Tested with VMS2.1 TACACS+ interoperability
IDS MC	Version 1.1	TACACS+ interoperability
LMS	—	TACACS+ interoperability (future release)
HSE	Version 1.7	TACACS+ interoperability
WLSE	—	TACACS+ interoperability (future release)

Table 12 PKI/Certificate Servers

Platform	Versions	Notes
Microsoft CA Certificate Server	Windows 2000 Windows 2000 with SP3	Tested

RQS Nº 03/2005 - CN
CPMI [redacted] 7 DS
0503
Fls:
Doc: 3701

Table 12 PKI/Certificate Servers (continued)

Entrust PKI	Version 6.0	—
Verisign Onsite	Version 5.0	—

Table 13 Token Servers[1]

Platform	Versions	Client Requirement	Notes
ActivCard Server	Version 3.1	—	—
CRYPTOCard CRYPTOAdmin	Version 5.16	—	—
PassGo Defender	Version 4.1.3	—	—
RSA ACE/Server	Version 5.1	—	Tested
Safeword Premier Access	Version 31.	—	—
Vasco Vacman Server	Version 6.0.2	—	—

1. Cisco Secure ACS Appliance uses a RADIUS interface to support all token servers. For more information, see Changes to Token Server Support.

Table 14 LDAP Servers

Platform	Versions	Notes
SunONE Identity Server (Formerly iPlanet Directory)	Version 5.1	Tested with Windows 2000 Active Directory with Windows Service Pack 3
Novell NetWare Directory Services (NDS)	Version 6.0	Tested
Novell eDirectory	Version 8.6	Tested

Table 15 User Databases[1]

Platform	Version	Requirement
SAM on Windows 2000	—	Tested with Service Pack 3

Table 15 User Databases[1] (continued)

AD on Windows 2000	—	—
SAM on Windows NT 4.0	—	—
LDAP	Generic	—
Novell NetWare Directory Services (NDS)	Version 6.0	Tested with eDirectory v.8.6 and Novell Client 4.83 SP2 for Windows NT 4.0, Windows 2000, and Windows XP
LEAP Proxy RADIUS servers	—	—

1. See also Table 13.

Table 16 Proxy Support

Platform	Versions	Notes
Cisco Secure ACS	2.4 or later	—
Funk Steel Belted Radius	Enterprise Edition	—

AP BF

~~RQS Nº 03/2005 - CN~~
CPMI - CORREIOS
Fls: 0505
Doc: 3701

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
Copyright © 2003, Cisco Systems, Inc.
All rights reserved.

ROS Nº 03/2005 - CN
CPMI - CORREIOS
0506
Fls:
3701
Doc:

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

Cisco Products Quick Reference Guide (CPQRG) **i**
- CPQRG Background **i**
- CPQRG Ordering Information **i**

How to Get More Complete Product Information **i**
Cisco Systems Overview **ii**
Cisco Channel Partner Program **iii**
- For More Information **iii**

Reseller and Customer Support **iii**
- Reseller Sales and Technical Assistance Contact Information **iii**
- Helpful Cisco Web Sites **iv**

Partner and Reseller Service and Support Offerings **v**
Product Warranty Information **vi**
Cisco Capital Financing **vi**
Cisco Authorized Refurbished Equipment (US and Canada Only) **vii**
Cisco Services **vii**

CHAPTER 1 Routers

Routers at a Glance **1-1**
- Sample Routing Solutions Overview—WAN & Internet Data Center **1-3**

Cisco Routers Port Matrix **1-4**
Memory Information for Routers **1-6**
Cisco SOHO Series Ethernet, ADSL over ISDN, ADSL and G.SHDSL Routers **1-8**
Cisco 800 Series **1-9**
Cisco 1700 Series **1-11**
Cisco 2500 Series **1-14**
Cisco 2600 Series **1-16**
Cisco 3600 Series **1-22**
Cisco 3700 Series **1-26**
Cisco 7200 Series **1-31**
Cisco 7300 Series **1-35**
Cisco 7400 Series **1-38**
Cisco 7500 Series **1-40**
Cisco 7600 Series **1-45**
Cisco 10000 Series **1-47**
Cisco 10720 Series **1-49**
Cisco 12000 Series **1-51**
Cisco SN 5400 Series Storage Router **1-55**

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0507
Fls:
3701

CHAPTER 2 **LAN Switching**

LAN Switching Products at a Glance **2-1**
Cisco LAN and MAN Products Port Matrix **2-2**
Cisco Catalyst 2900 Series **2-3**
Cisco Catalyst 2900 Series XL—Modular Switches **2-4**
Cisco Catalyst 2950 Series Intelligent Ethernet Switches **2-6**
Cisco Catalyst 3500 Series XL **2-10**
Cisco Catalyst 3550 Series Intelligent Ethernet Switches **2-12**
Cisco Catalyst 4500 Series **2-15**
Cisco Catalyst 4000 Series — Fixed Configuration **2-17**
Cisco Catalyst 5000 Family **2-18**
Cisco Catalyst 6500 Family **2-20**
Cisco Catalyst 8500 Multiservice Switch Routers **2-24**

CHAPTER 3 **Wireless LAN Products**

Wireless LAN Products at a Glance (IEEE 802.11b) **3-1**
Sample Wireless LAN Solution Overview—In-Building or Site-to-Site **3-2**
Cisco Aironet 1200 Series Access Points **3-2**
Cisco Aironet 1100 Series Access Points **3-5**
Cisco Aironet 5 GHz 54 Mbps Wireless Client Adapter **3-6**
Cisco Aironet 350 Series Client Adapters **3-8**
Cisco Aironet 350 Series Workgroup Bridge **3-10**
Cisco Aironet 350 Series Wireless Bridge **3-12**
Cisco Aironet Antennas and Accessories **3-14**

CHAPTER 4 **IP Telephony, Video, & Web Collaboration**

Campus IP Telephony, Video, & Web Collaboration at a Glance **4-1**
Cisco 7900 Series IP Phones **4-3**
Cisco CallManager 3.3 **4-4**
Cisco IP Contact Center (IPCC) Enterprise Edition **4-8**
Cisco IPCC Express Edition (Formerly IP ICD) **4-9**
Cisco IP IVR **4-10**
Cisco Unity—Unified Messaging and Voice Mail **4-11**
Cisco Personal Assistant **4-13**
Additional Cisco IP Telephony Applications **4-14**
- Cisco SRS Telephony **4-14**
- Cisco IP Phone Messenger **4-15**
- Cisco IP SoftPhone **4-15**
- Cisco IP Manager Assistant **4-15**
- Cisco Conference Connection **4-16**

Cisco MCS 7800 Series Media Convergence Servers **4-17**
- Cisco MCS 7815I-2000 **4-17**
- Cisco MCS 7825H-2266 **4-17**
- Cisco MCS 7835H-2400 and Cisco MCS 7835I-2400 **4-17**
- Cisco MCS 7845H-2400 and Cisco MCS 7845I-2400 **4-17**

Cisco ICS 7750 Integrated Communications System **4-18**
Cisco IAD 2400 Series Integrated Access Device with IOS Telephony Service (ITS) **4-21**
Cisco Voice Gateways **4-22**
- Cisco VG248 Voice Gateway **4-22**

Cisco IP/VC 3500 Series Videoconferencing Products **4-22**
Cisco IP/TV 3.4 **4-23**

Web Collaboration—Cisco Web Collaboration Option **4-24**
E-Mail Response Management—Cisco E-mail Manager **4-25**
Cisco Emergency Responder **4-25**
Cisco ATA Series of Analog Telephone Adaptors **4-27**

CHAPTER 5 **VPN and Security Products**

VPN and Security Products at a Glance **5-1**
Cisco PIX Firewall Series **5-2**
Cisco IOS Firewall **5-5**
Cisco VPN 3000 Family **5-6**
Cisco Intrusion Detection System Network Sensors **5-8**
Cisco Security Agent **5-10**
Cisco 7100 Series **5-11**
Cisco Secure Access Control Server for Windows **5-14**
Cisco Secure User Registration Tool **5-15**

CHAPTER 6 **Content Networking Products**

Content Networking Products at a Glance **6-1**
Content Networking Overview **6-2**
Cisco Content Engines **6-2**
Cisco CSS 11500 Series Content Services Switches **6-4**
Cisco LocalDirector **6-6**
Cisco Content Distribution Manager 4600 Series **6-7**
Cisco Content Router 4430 **6-9**
Cisco Content Switching Module **6-10**
Cisco SSL Module for Catalyst 6500 **6-11**
Cisco 11000 Series Secure Content Accelerator (SCA 11000) **6-12**
Cisco CTE-1400 Series Content Transformation Engine **6-13**
Cisco DistributedDirector **6-14**
Cisco GSS 4480 Global Site Selector **6-15**

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 0508
Doc: 3701

CHAPTER 7 Broadband and Dial Access Products

Broadband and Dial Access Products at a Glance **7-1**
- Remote Dial Access—Data and Voice (VoIP) **7-1**
- Broadband Cable **7-1**
- DSL (Digital Subscriber Line) Access **7-2**
- ATM Multiservice WAN Switching **7-2**
- Long Reach Ethernet **7-3**

Memory Information for Access Routers **7-3**
Cisco AS5350 Universal Gateway **7-3**
Cisco AS5400 Series Universal Gateways **7-6**
Cisco AS5850 Universal Gateway **7-9**
Remote Dial Access Network Management Products **7-11**
- Universal Gateway Manager (UGM) **7-11**
- Cisco Universal Gateway Call Analyzer **7-11**
- Cisco Resource Policy Management System **7-12**

SS7 Signaling & Softswitch Products **7-12**
- Cisco SC2200 Signaling Controller **7-12**
- Cisco PGW 2200 Softswitch **7-12**
- Cisco BTS 10200 Softswitch **7-13**

Additional Remote Dial Access Products **7-13**
Cisco uBR7100 Series Universal Broadband Router **7-13**
Cisco uBR7246VXR Universal Broadband Router **7-15**
Cisco uBR10012 Universal Broadband Router **7-16**
Cisco RF Switch **7-17**
Broadband Cable—Customer Premise Equipment (CPE) **7-19**
- Cisco uBR900 Series Cable Access Routers **7-19**

Remote Cable Access—Network Management Products **7-20**
- Cisco Cable Manager **7-20**
- Cisco Cable Diagnostic Manager **7-20**
- Cisco Broadband Troubleshooter **7-20**
- Cisco Broadband Configurator **7-21**

DSL Remote Access—Customer Premise Equipment (CPE) **7-21**
Broadband Services Aggregation **7-21**
- Cisco 7200 Series **7-22**
- Cisco 7301 Series **7-22**
- Cisco 7400 Series **7-22**
- Cisco 10000 Series **7-22**
- Cisco 6400 Series **7-23**

ATM Multiservice WAN Switching **7-23**
Cisco BPX 8600 Series—Advanced ATM Multiservice Switches **7-23**
Cisco MGX 8850 ATM Multiservice Switch **7-24**
Cisco MGX 8830 ATM Multiservice Switch **7-25**
Cisco MGX 8200 Series **7-25**
- Cisco MGX 8230 Edge Concentrator **7-25**
- Cisco MGX 8250 Edge Concentrator **7-25**

Cisco IGX 8400 Series Multiservice WAN Switch **7-25**
Cisco Long Reach Ethernet Solution **7-26**
- Catalyst 2950 LRE Series Intelligent Ethernet Switches **7-26**
- Cisco 575 and 585 LRE CPE Devices **7-27**
- Cisco LRE 48 POTS Splitter **7-27**

Cisco Building Broadband Service Manager (BBSM) Version 5.2 **7-28**
Cisco BBSM Hotspot Server Version 1.0 **7-29**
Sample LRE Solution Overview—Broadband Internet Access for MxU **7-29**

CHAPTER 8 **Optical Transport**

Optical Transport Products at a Glance **8-1**
Sample Metro Optical Transport Solution Overview— Delivering Multiservices to the Edge **8-2**
Cisco ONS 15200 Optical Metro DWDM Series **8-3**
Cisco ONS 15302/15305 SDH Multiservice CPE & Aggregation Platforms **8-3**
Cisco ONS 15454 and 15327 Multiservice Provisioning Platforms **8-4**
Cisco ONS 15501 Erbium Doped Fiber Amplifier **8-5**
Cisco ONS 15530 **8-5**
Cisco ONS 15540 Extended Services Platform (ESPx) **8-6**
Cisco ONS 15600 Multiservice Switching Platform **8-7**
Cisco Transport Manager (CTM 4.x) (Element/Network Management) **8-8**

CHAPTER 9 **IOS Software & Network Management**

Cisco IOS® Software & Network Management Products at a Glance **9-1**
CiscoWorks for Windows **9-2**
Cisco IOS® Software **9-4**
Quality of Service (QoS) **9-4**
Converged LAN/WAN and Telephony Networks **9-5**
Security **9-5**
Cisco IOS NetFlow **9-6**
Cisco IOS Routing Services **9-6**
IP Routing Protocols **9-6**
Multi Protocol Label Switching (MPLS) **9-6**
IP Multicast and Multicast Solutions **9-8**
IPv6 **9-10**
Cisco IOS Software Release Process **9-10**
Cisco Network Management Overview **9-11**
Cisco Network Management Products **9-11**
CiscoWorks Small Network Management Solution **9-11**
CiscoWorks Small Network Management Solution Components **9-12**
CiscoWorks Routed WAN Management Solution **9-13**
CiscoWorks LAN Management Solution **9-14**
CiscoWorks VPN/Security Management Solution **9-16**
CiscoWorks IP Telephony Environment Monitor **9-18**
CiscoWorks Voice Manager for Voice Gateways **9-19**
CiscoWorks QoS Policy Manager **9-21**
Cisco Ethernet Subscriber Solution Engine **9-22**
CiscoWorks Wireless LAN Solution Engine **9-23**
CiscoWorks Hosting Solution Engine **9-24**
Cisco Catalyst 6500 Series Network Analysis Module 1 and 2(with NAM software version 2.2) **9-25**

ECT 3782
RQS Nº 03/2005 - CN
CPMI - CORREIOS
0509
Fls:
Doc: 3701

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.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0510
Fls:
Doc: 3704

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

ROS Nº 03/2005 - CN
CPMI - CORREIOS
0511
Fls:
3701
Doc:

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.cisco.com/login
Partner Help Search partners' frequently asked questions and ask for the help you need	http://ciscopartner.custhelp.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/GetLogin.jsp?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/GetLogin.jsp?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)

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0512
Fls:
Doc: 3701

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 shipping within 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-free and the SW conforms to its published specifications • Guest Access to Cisco Connection Online (CCO)
90-Day Limited Hardware Warranty(78-5236-vvrr)	• Advance Replacement shipping within 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-free and the SW conforms to its published specifications • Guest Access to Cisco Connection Online (CCO)
One-Year Limited Hardware Warranty (78-10747-vvrr)	• Advance Replacement shipping within 10 business days from RMA date within One Year of original shipment from Cisco or from Cisco Reseller • 90-Day Assurance that the Media SW is delivered is defect-free and the SW conforms to its published specifications • Guest Access to Cisco Connection Online (CCO)
Limited Lifetime Hardware Warranty (78-6310-vvrr)	• Advance Replacement shipping within 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-free and the SW conforms to 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-free and the SW conforms to 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)	• Replacement shipping 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/qrdering/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

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0513
Fls:
Doc 3701

CHAPTER 1

Routers

Routers at a Glance

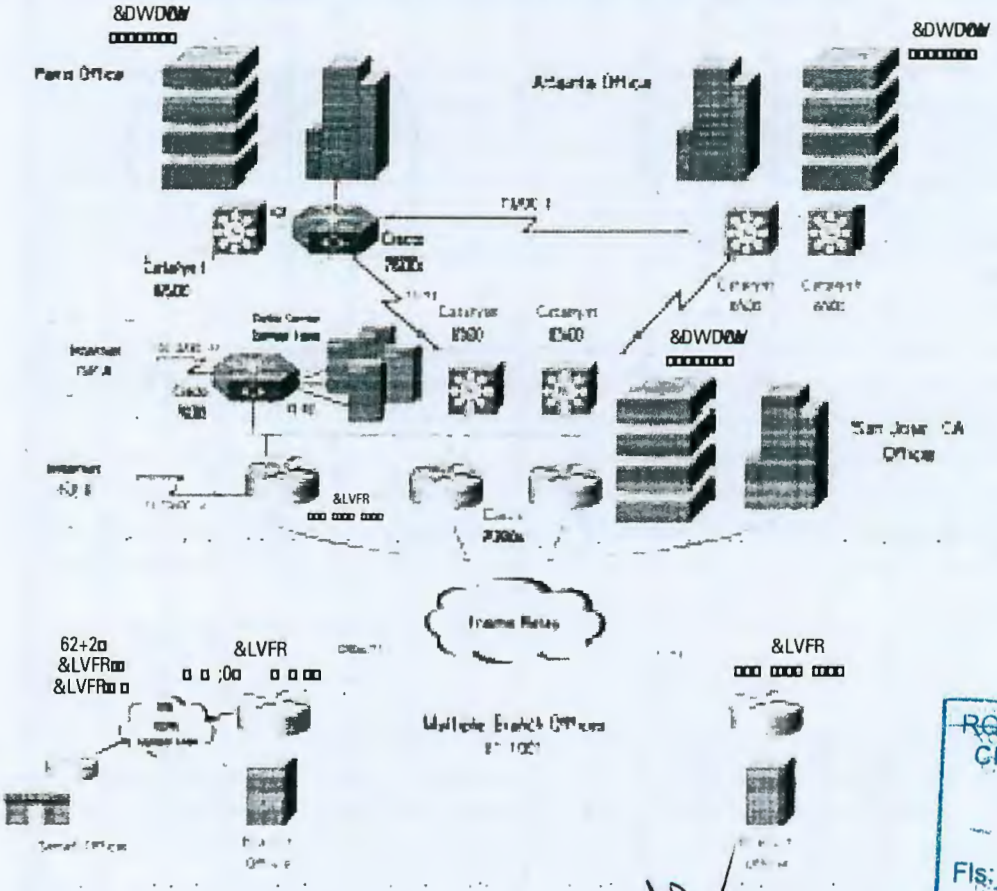
Product	Features	Page
Cisco IOS® Software	See the Chapter 9—Cisco IOS Software and Network Management for an overview of Cisco IOS Software	9-4
Cisco SOHO Series Secure Broadband Routers	Ethernet, ADSL, ADSL over ISDN, and G.SHDSL Routers for Small Office and Home Ofices • Integrated security of Cisco 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 security features including stateful inspection 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 Capability • Supports up to three Ethernet connections with 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 line 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, Ethernet, 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 Cisco 3640A as an alternative for customers with configurations not available on the Cisco 3700.	1-22

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0514
Fls:
3701
Doc:

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 intelligent 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 performance 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 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



ROS Nº 03/2005 - CN
CPMI - CORREIOS
0515
Fls:
Doc: 3701

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

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0516
Fls:
Doc:
3701

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 and 4MB 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 and 4MB 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	Default 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	

ECT 3760 21 ...ED

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0517
Fls:
Doc:
3701

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 1 G.SHDSL port with firewall security and Cisco IOS manageability 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 Specifications for 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

ROS Nº 03/2005 - CN
CPMI - CORREIOS
0518
Fls:
3701
Doc:

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 functionality in one device when connecting to the Internet using a broadband modem • Hardware-assisted 3DES VPN encryption at full T1/E1 speeds
Cisco 1721	• Secure data-only access solution that adapts to customers' evolving network requirements • Support for data applications including 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 and digital 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

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0519
Fls:
Doc: 3701

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	12.1 Mainline	4 MB	16 MB
	IP/ADSL		8 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 Security Access 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 (dial and leased line)
WIC-1B-U	1-port BRI w/ NT-1 WAN Interface Card (dial and 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—BRI (NT & TE)
VIC-2FXO-M1	2-port FXO for U.S. with battery reversal
VIC-2FXO-M2	2-port FXO for Europe with battery reversal
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

3762

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 0520
Doc: 3701

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 (depending on 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 x 5 x NBD) for the Cisco AS2509 and AS2511

For More Information

See the Cisco 2500 Series Web site: **http://www.cisco.com/go/2500**

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0521
Fls:
3701
Doc:

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 higher level of performance for a broadened range of concurrent remote office applications, including unparalleled voice/data integration, Virtual Private Network (VPN) performance, increased bandwidth to support voice and video applications, and the delivery of Web-based applications.
Cisco 2600XM Series	• Enterprises considering the Cisco 2600 for branch office applications should 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 Dual 10/100 Modular Router with Cisco IOS IP
Cisco 2650XM	• High performance 10/100 Modular Router with Cisco IOS IP
Cisco 2621XM	• Mid Performance Dual 10/100 Ethernet Router with Cisco IOS IP
Cisco 2620XM	• Mid Performance 10/100 Ethernet Router with Cisco IOS IP
Cisco 2611XM	• Dual 10/100 Ethernet 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 for mixed LANs and migrating from Token Ring to Ethernet

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 Pathbuilder S400
- 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

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0522
Fls:
Doc: 3701

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/ Cisco IOS 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 Performance 10/100 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 Dual 10/100 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/Cisco IOS IP-DC NEBs
CISCO2650XM-RPS	High Performance 10/100 Modular Rout w/Cisco IOS IP-RPS ADPT
CISCO2651XM	High Performance Dual 10/100 Modular Rout with Cisco IOS 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 configured 2600 for FIPS
C2651XM-2FE/VPN/K9	2651XM/VPN Bundle, AIM-VPN/EP/2FE/IDS 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 (Dial and Leased Line)
WIC-1B-U-V2	1-port BRI (U) w/NT-1 WAN Interface Card (Dial and 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 channel voice/fax network 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 channel voice/fax network 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

ECT COMLA

ROS Nº 03/2005 - CN
CPML - CORREIOS
0523
Fls:
3701
Doc:

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 Interface Card (for Europe)
VIC-2FXO-M3=	2-port FXO Voice Interface Card (for Australia)
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) network module
NM-8B-S/T=	8-port BRI (S/T) network module
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 network module

Cisco 2600/2600XM and 3600 Series Network Modules (International)

NM-1CE1B=	1-port Channelized E1/ISDN-PRI balanced network module
NM-1CE1U=	1-port Channelized E1/ISDN-PRI unbalanced network module
NM-2CE1B=	2-port Channelized E1/ISDN-PRI balanced network module
NM-2CE1U=	2-port Channelized E1/ISDN-PRI unbalanced network module

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 AIM for 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 Cisco 2600 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**

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0524
Fls:
Doc: 3701

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 connectivity • 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 Numbers and Ordering Information	Same as Cisco 3620	Same as Cisco 3620
WAN Modules	See Part Numbers and Ordering Information	Same as Cisco 3620	Same as Cisco 3620 (Hardware compression support only through AIM-COMPR4)
ATM Modules	See Part Numbers and Ordering Information	Same as Cisco 3620	Same as Cisco 3620
Voice/Fax Network Modules	See Part Numbers and Ordering Information	Same as Cisco 3620	Same as Cisco 3620
WAN Interface Card (WIC) Modules	See Part Numbers and Ordering Information	Same as Cisco 3620	Same as Cisco 3620
Multiflex Voice/WAN Interface Cards	See Part Numbers and Ordering Information	Same as Cisco 3620	Same as Cisco 3620
Voice Interface Card (VIC) Modules	See Part Numbers and Ordering Information	Same as Cisco 3620	Same as Cisco 3620
Modem Modules	See Part Numbers and 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); 64 MB (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

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0525
Fls: 3701
Doc:

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

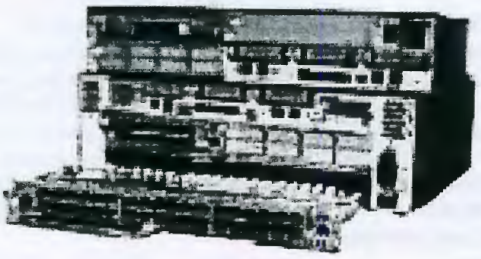
Cisco 3600 Series Accessories	
ACS-3620RM-19=	Cisco 3620—19-Inch Rack Mount Kit
ACS-3620RM-24=	Cisco 3620—24-Inch Rack Mount Kit
PWR-3620-AC	Cisco 3620—AC Power Supply
PWR-3620-DC	Cisco 3620—DC Power Supply
ACS-3620RPS=	Cisco 3620—RPS Field Upgrade
ACS-3640RM-19=	Cisco 3640—19-Inch Rack Mount Kit
ACS-3640RM-24=	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 SMARTnet Maintenance 8x5xNBD
CON-SNT-PKG13	Cisco 3661 and Cisco 3662 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).
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 flexible 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 digital 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

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 0527
Doc: 3701

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 Software
CISCO3745	4-slot Modular Multiservice Router with IP Software

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 speed serial 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 Ethernet 2 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 Ethernet 2 WAN Card Slot Network Module
NM-1FE-FX	1-port Fast Ethernet network module (10/100Base Fiber only)

E C T 3746 2 C P I - C

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 (supports 30 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) Supports add/drop multiplexing (drop and insert)
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 (supports 24 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) Supports add/drop multiplexing (drop and insert)
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 network module
NM-2V	2-slot voice and fax network 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 battery reversal, for North America)
VIC-2FXO-M2	2-port voice interface card—FXO (with battery reversal, for Europe)
VIC-2FXO-M3	2-port voice interface card—FXO (for Australia)
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

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 0528
3701
Doc:

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 network module
NM-1CE1U	1-port channelized E1/ISDN PRI unbalanced network module
NM-2CE1B	2-port channelized E1/ISDN PRI balanced network module
NM-2CE1U	2-port channelized E1/ISDN PRI unbalanced network module
NM-4B-S/T	4-port ISDN BRI network module
NM-4B-U	4-port ISDN BRI with NT1 network module
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 network module
NM-18DM	18-port digital modem network module
NM-24DM	24-port digital modem network module
NM-30DM	30-port digital modem network module
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 AIM for 3660-High Performance
AIM-VPN/EPDES/3DES	VPN Encryption AIM for 2600-Enhanced Performance
Content Engine Network Modules	
NM-CE-BP-20G-K9	Content Engine Network Module, Basic Performance, 20GB IDE Hard Disk
NM-CE-BP-40G-K9	Content Engine Network 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 with Inline Power and GE
PPWR-DCARD-16ESW	One Inline power daughter card for 16 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 with Inline Power
NMD-36-ESW-2GIG	One 36 port 10/100 EtherSwitch HDSM with two 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 bus for 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 bus for 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

ECT 3700 CPL-AS
ROS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 0529
Doc: 3701

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 (expandable to 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 specified 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 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 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) 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 Adapter 4E1 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 multichannel T1/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-reach port adapter
PA-SRP-OC12SMX=	DPT-OC12 Singe-mode extended reach PA

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0530
Fls:
Doc: 3701

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 Adapter with 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 T3 port adapter
PA-MC-E3=	1 port Multi-Channel E3 port adapter
PA-MC-4T1=	4 port multichannel T1 port adapter with integrated CSU/DSUs
PA-MC-2T3+=	2 port multichannel T3 port 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 Adapter with E3 DSU
PA-A3-T3=	1-Port ATM Enhanced DS3 Port 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 Adapter with 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 Adapter with 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 Adapter with 30 Channels
PA-VXA-1TE1-24+=	1 Port T1/E1 Digital Voice Port Adapter with 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 Converter for 1000BASE-LX standard
GBIC-SX=	Gigabit Intf. Converter For 1000BASE-SX (Short Wavelength)
GBIC-ZX=	Gigabit Interface Converter for 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

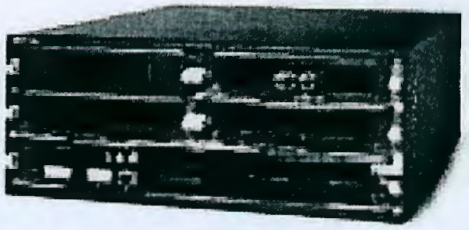
Cisco 7200 Series Power Supplies	
PWR-7200-DC+=	Cisco 7200 DC (24V-60V) Power Supply Option
PWR-7200/2-DC+	Cisco 7200 Dual DC (24V-60V) Power Supply Option
PWR-7200-AC=	Cisco 7200 AC Power Supply With United States Cord
PWR-7200-ACA=	Cisco 7200 AC Power Supply With Australian Cord
PWR-7200-ACE=	Cisco 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 optimized 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

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0531
Fls:
Doc:
3701

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 (expandable to 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 Cisco 7304 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 Cisco 7304 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. Converter For 1000BASE-SX (Short Wavelength)
GBIC-ZX=	Gigabit Interface Converter for 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

E C T 3738 CPI - RS

RQS Nº 03/2005 - CN CPMI - CORREIOS 0532 Fls: Doc: 370

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 SX transceiver
GLC-LH-SM=	GE SFP, LC connector LH transceiver

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 broadband subscriber services suite with highest subscribers per rack ratio • One fast LAN interface (FE/GE) and one fast WAN interface (DS3/OC3) • High volume/density of 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 to 512MB)	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 Converter for 1000BASE-LX standard
GBIC-SX=	Gigabit Intf. Converter For 1000BASE-SX (Short Wavelength)
GBIC-ZX=	Gigabit Interface Converter for 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

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 0533
Doc: 3701

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 Converter for 1000BASE-LX standard
GBIC-SX=	Gigabit Intf. Converter For 1000BASE-SX (Short Wavelength)
GBIC-ZX=	Gigabit Interface Converter for 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 power supplies • Diverse set of routing protocols (all platforms)
Cisco 7513	• 13 expansion slots • Dual CyBuses • Redundant power supplies • Diverse set of routing protocols (all platforms)

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
- Juniper: M5, M10, M20
- Unisphere: ERX700, ERX1400
- 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.

RQS Nº 03/2005 - CN - CPMI - CORREIOS
0534
Fls:
Doc: 3701

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

ECT 337 APL-AC

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. Converter For 1000BASE-SX (Short Wavelength)
GBIC-LX/LH=	Gigabit Interface Converter for 1000BASE-LX standard
GBIC-ZX=	Gigabit Interface Converter for 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

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0535
Fls:
3701

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 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 Enterprise
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)

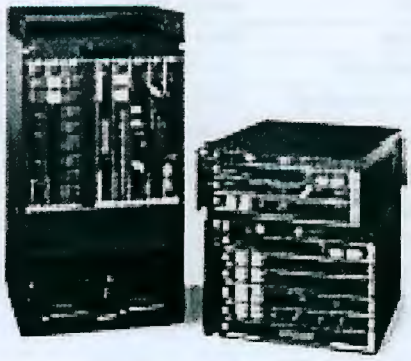
PA-MC-8TE1+=	8 port multichannel T1/E1 8PRI port adapter

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
- Juniper: M5, M10, M20, M40
- Unisphere: ERX700, ERX1400
- Extreme: Black Diamond 6808

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0536
Fls:
3701
Doc:

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 to 512MB)	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-POS-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 Ethernet Optical 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 4 GE
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

ECT 3726 DSL-AC
Fls: 0537
Doc: 3701
CPMI - CORREIOS
N° 03/2005 - CN

- 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

ECT 3226 28 CPL AC

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 power entry 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 channel E3/DS3 Line Card
ESR-6CT3	6 port channelized T3 line card
ESR-1GE	1 pt Gigabit Ethernet line card (requires a GBIC)
ESR-GBIC-SX	1000base-SX GBIC, multimode,standardized for ESR
ESR-GBIC-LHLX	1000base-LH GBIC,singlemode,standardized for 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.

RQS Nº 03/2005 - CN - CPMI - CORREIOS 0538 Fls 3701

When to Sell

Sell This Product	When a Customer Needs These Features
Cisco 10720 Internet Router	• Any service provider planning to offer high-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 the simple, 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 Services such as L2 and L3 VPN with FE/GE hand off 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 Cisco Discovery Protocol (CDP) Serial (aux) and console ports 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—modules are not interchangeable or hot swappable: • Upper slot is dedicated for DPT or POS Uplink module equipped with two 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 upper slot is the CON-AUX module, which is a depopulated uplink card 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 for 24-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 connectors while the FX-SM and FX-MM modules are equipped with MT-RJ connectors. • Also available is a combination 4 Gigabit Ethernet with 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 deployments within 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

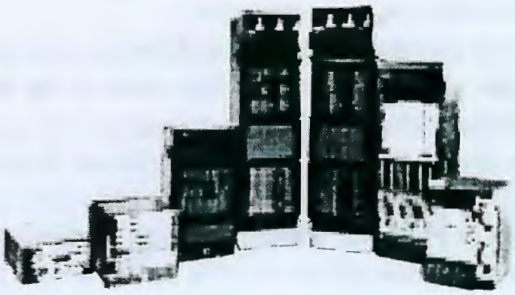
CISCO10720-AC-A	Cisco 10720 Internet Router with dual AC power supply
CISCO10720-DC-A	Cisco 10720 Internet Router with dual DC Power Supply
10720-FE-TX	24-port 10/100 Ethernet Access Module—RJ45 connectors
10720-FE-FX-MM	24-port 100Mbps Multimode Fiber Ethernet Access Module 2km—MTRJ connectors
10720-FE-FX-SM	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.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0539
Fls:
3701
Doc:

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 • Support for high-density, high-speed interfaces: ATM, DPT/RPR, POS, GbE/FE ranging from channelized DS3 (to DS1) through OC-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 applications like voice and video • Support for IP or MPLS forwarding • Support for hundreds of thousands of routes • Proven carrier- class reliability and availability through enhanced features 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 • Support for high-density, high-speed interfaces: ATM, DPT/RPR, POS, GbE/FE ranging from channelized DS3 (to DS1) through OC-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 upgradeable to 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 solution to 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[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

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0540
Fls:
3701
Doc:

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
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/SDH Single-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 T3 for the GSR
GLC-LH-SM	GE SFP, LC connector LH transceiver
GLC-SX-MM	GE SFP, LC connector SX transceiver
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 connector type, 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.

ECT 3720 CPL-AC

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

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0541
Fls:
Doc: 3701

Selected Part Numbers and Ordering Information[1]

Cisco SN 5428 Storage Router

SN5428	The SN 5428 provides two Gigabit Ethernet ports, supporting iSCSI, for connection to standard IP networks and eight Fibre Channel fabric 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-PKG*10*	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

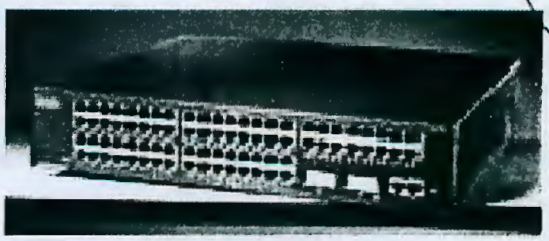
RQS Nº 03/2005 - CN
CPMI - CORREIOS
0542
Fls:
3701
Doc:

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

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0543
Fls:
3701
Doc:

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

RQS Nº 03/2005 - CPMI - CORREIOS
Fls: 0544
Doc: 3701

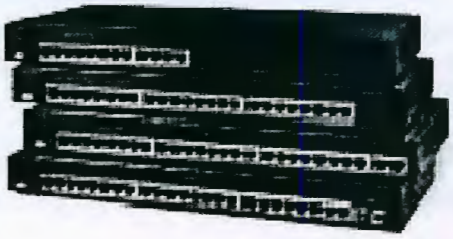
Catalyst 2900 Series XL Packaged SMARTnet Maintenance 8x5xNBD	
CON-SNT-PKG4	Catalyst 2900 Series WSC2924M-XL-EN Packaged SMARTnet 8x5xNBD
CON-SNT-PKG5	Catalyst 2900 Series WSC2924M-XL-EN-DC Packaged SMARTnet 8x5xNBD
CON-SNT-PKG7	Catalyst 2900 Series WSC2912MF-XL Packaged SMARTnet 8x5xNBD

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

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0545
Fls:
3701
Doc:

- 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

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

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0546
Fls:
3709
Doc:

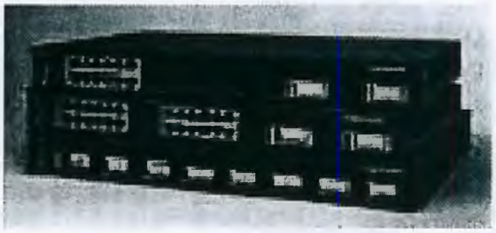
Redundant Power System (RPS)	
PWR675-AC-RPS-N1=	675W Redundant Power Supply with 1 connector cable
CAB-RPS-1414=	1.2 meter cable for Cisco RPS 300 to external device connection
Cables/Accessories	
CAB-RPS-1614=	1 RPS 675 connector cable 16/14
CAB-GS-50CM	50 centimeter cable for GigaStack GBIC
STK-RACKMOUNT-1RU=	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, Alarms, 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**

ECT 3708 CPMI-CORREIOS
ROS Nº 03/2005 - CN
CPMI - CORREIOS
0547
Fls:
Doc: 370

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 advanced IP 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 advanced IP 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 advanced IP routing • Medium Port Density • Integrated inline power 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 inline power 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 advanced IP 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 advanced IP 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 (requires EMI), 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

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0548
Fls:
3701
Doc:

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 Ethernet ports; 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 (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 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**

C T 3204

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

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0549
Fls:
Doc 3701

- 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, BigIron 4000
- 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 uplink ports on Supervisor Engine II, III and 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 Supply with Int Voice
PWR-C45-2800ACV=	Catalyst 4500 2800W AC Power Supply with 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

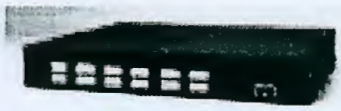
Catalyst 4500 Series Line Card Modules and GBICs	
WS-X4124-FX-MT=	Catalyst 4000 FE Switching Module, 24-port 100FX (MTRJ)
WS-X4148-FX-MT=	Catalyst 4000 FE Switching Module, 48-100FX MMF (MTRJ)
WS-X4148-RJ=	Catalyst 4000 10/100 Fast Ethernet Module, 48 Ports (RJ-45)
WS-X4148-RJ21=	Catalyst 4000 Telco 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

ECT 3702 20 - AC

ROS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 0550
Doc: 3701

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 centre or 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 Numbers and 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).

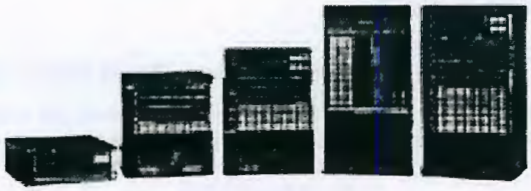
For More Information

See the Catalyst 5500/5000 series Web site: **http://www.cisco.com/go/5000**

ECT 3700 20 PLIAS

BOS Nº 03/2005 - CN - CPMI - CORREIOS
Fls: 0551
Doc: 3701

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 platform that meets requirements for a dynamic environment including very high multilayer switching performance with high Fast Ethernet and Gigabit Ethernet port densities
Catalyst 6500 Family Solutions	• Enterprise campus distribution and core—With industry-leading port densities, performance, and high availability solutions • Enterprise Server Farm—For Gigabit wire-speed access to mission-critical server farms • High-capacity wiring 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 integrated platform simplifies network design, decreases rack space requirements, and decreases overall administration costs • Advanced, integrated hardware based firewall, content switching, intrusion detection, and network analysis capabilities • 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

ECT 3698 1 20 CPL - AC

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 (cable included)
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

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0552
Fls:
Doc: 3701

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 Ethernet Module, 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 (MSFC)II, 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 SMARTnet Maintenance 8x5xNBD
CON-SNT-PKG14	Catalyst 6506 L2 Bundle SMARTnet Maintenance 8x5xNBD .
CON-SNT-PKG15	Catalyst 6509 L2 Bundle SMARTnet Maintenance 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**

ECT 3696 CPL-AC

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0553
Fls:
Doc: 3701

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 4 Clock Module—AC Power (also available in DC Power)
C8545MSR-MRP4CLK=	C8540 MSR Multiservice Route Processor (spare)
C8545MSR-MRP3CLK=	C8540 MSR Route Processor Stratum 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 (also available 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) (also available 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 Enhanced ATM Router Module (spare)
Catalyst 8500—Layer 3 Modules and ATM Interface Modules and Uplinks	
C85EGE-2X-16K=	C8540 2-port Enhanced GE 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 Ethernet 16K (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 EI and in 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**

ECT 3684 30 OPL-AC

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0554
Fls:
Doc: 3701

CHAPTER 3

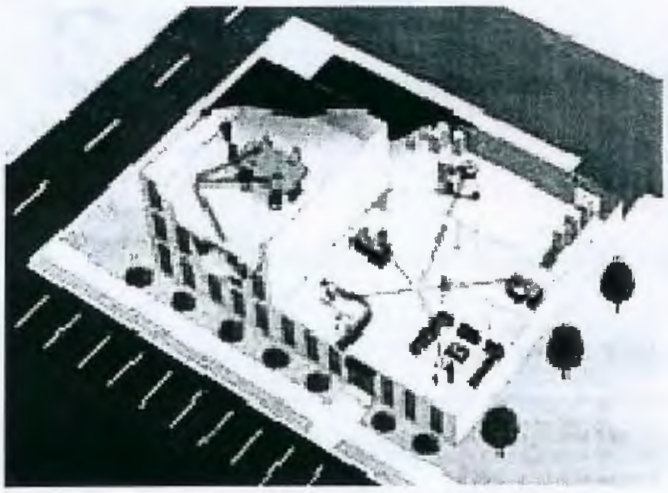
Wireless LAN Products

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 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 local power	3-2
Cisco Aironet 1100 Series Access Point	• Single 802.11b radio, upgradable to 802.11g • Provides end-to-end solution support for Intelligent Network Services • 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 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	3-6
Cisco Aironet 350 Series Client Adapters	• Superior range and throughput • Secure network communications • World mode for international roaming • 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 point-to-point and point-to-multipoint configurations • Broad range of support antennas • Simplified installation, improved performance, and upgradeable firmware, 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 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

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 0555
Doc: 3701

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	Indoor: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)

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0556
Fls:
3701
Doc:

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**

ECT 3689 20 PL-IAC

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

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0557
Fls:
Doc: 3704

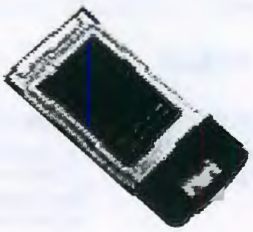
Feature	Cisco Aironet 1100 Series Access Points
Available Transmit Power Settings[1]	100 mW (20 dBm); 50 mW (17 dBm); 30 mW (15 dBm); 20 mW (13 dBm); 5 mW (7 dBm); 1 mW (0 dBm) Maximum power setting will vary according to individual country regulations
Range (typical @ maximum power setting, 2.2 dBi 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.

ECT 3687 20 ABL-AC

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

RQS Nº 03/2005 - CN CPMI - CORREIOS 0558 Fls: 3701 Doc:

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 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.

RQS Nº 03/2005 - CPMI - CORREIOS
0559
Fls:
Doc: 3701

Selected Part Numbers and Ordering Information[1]

Cisco Aironet 350 Series Client Adapters

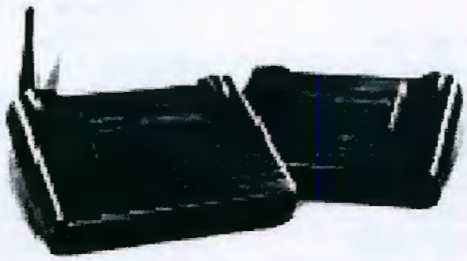
AIR-PCM352	350 Series PC Card with Diversity Antennas & 128-bit WEP
AIR-PCI352	350 Series PCI Card with 2.2 dBi Dipole Antenna & 128-bit WEP

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	• 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)

ANATEL 3683 22

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**

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 3701
Doc:

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**

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0560
Fls:
Doc:
3701

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

C T
3679
2l
L - A C

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.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 0561
Doc: 3701

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

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0562
Fls:
3701
Doc:

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

ROS Nº 03/2005 - CN CPMI - CORREIOS Fls: 0563 Doc: 3701

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 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

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0564
Fls:
Doc: 3701

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**

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0565
Fls:
3701
Doc:

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

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0566
Fls:
Doc: 3701

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.

ECT 3667 20
ROS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 0567
Doc: 3701

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.

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**

C T 3665 1 L-AC

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

RQS Nº 03/2005 - CN CPMI - CORREIOS 0568 Fls: Doc: 3701

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**

3663

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.

RQS Nº 03/2005 - C
CPMI - CORREIOS
Fls: 0569
3701
Doc:

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

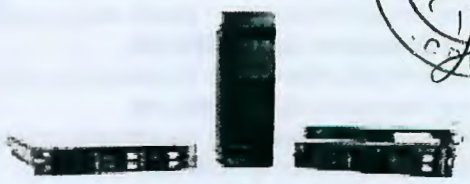
Cisco Conference Connection (CCC) is designed for small to medium enterprises and remote offices of larger enterprises. Cisco Conference Connection facilitates relevant participation regardless of location, enables faster decisions, and eliminates travel cost and time and disruptions caused by requirements 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	Intel Pentium® 2266-MHz processor 512KB L2 CacheSDRAM is configuration dependant	Intel Xeon® 2400-MHz processor 512KB Cache	Intel Xeon® 2400-MHz processor 512KB Cache	Dual Intel Xeon® 2400-MHz processor 512KB Cache	Dual Intel Xeon® 2400-MHz processor 512KB Cache
512MB SDRAM	Hard Disk is configuration dependant	SDRAM is configuration dependant	SDRAM is configuration dependant	SDRAM is configuration dependant	SDRAM is configuration dependant
40GB ATA/100 Hard Disk	1.44MB Floppy Disk	Hard Disk is configuration dependant	Hard Disk is configuration dependant	Hard Disk is configuration dependant	Hard Disk is configuration dependant
1.44MB Floppy Disk	DVD Drive	SCSI Controller.	SCSI Controller.	SCSI Controller.	SCSI Controller.
DVD Drive	Hard Disk Controller is configuration dependant	Dual 10/100/1000 Ethernet NIC2U Rack Mount System.	Dual 10/100/1000 Ethernet NIC2U Rack Mount System	Dual 10/100/1000 Ethernet NIC2U Rack Mount System	Dual 10/100/1000 Ethernet NIC2U Rack Mount System
Integrated ATA Controller	Dual 10/100/1000 Ethernet NIC1U Rack Mount System				
Single 10/100/1000 Ethernet NIC					
Tower System with optional rack mount kit.					

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0570
Fls:
3701
Doc:

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 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; Cisco Media Convergence Server 7845H-2400
MCS-7845H-2.4-ECS1; MCS-7845H-2.4-ECS2

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

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0571
Fls:
Doc: 3701

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**

ECT 3657 GPL-AS

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**

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0572
Fls:
3701
Doc:

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.

C T 3655 1 - AC

- 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.

RQS Nº 03/2005 - CN - CPMI - CORREIOS 0573 Fls: 3701 Doc:

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.

RQS Nº 03/2005 - CPMI - CORREIOS
0574
Fls:
Doc: 37

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

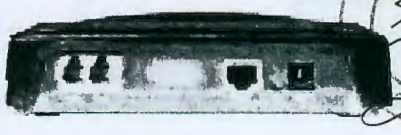
SW-ER1.1-SVR	Cisco Emergency Responder software (MCS platforms), including 100 user licenses
SW-ER1.1-SVR-CPQ=	Cisco Emergency Responder software (Compaq platforms), including 100 user licenses
SW-KEY-ER1.1-USER=	Incremental single-user license key for Cisco Emergency Responder

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

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0575
Fls:
3701

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

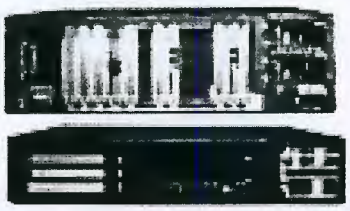
VPN and Security Products at a Glance

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

RQS Nº 03/2005 - CPMI - CORREIOS
Fls: 0576
Doc: 3701

Product	Features	Page
Cisco Secure Access Control Server (ACS) for Windows	Controls the authentication, authorization, and accounting (AAA) of users and administrators 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	to 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

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0577
Fls:
3701
Doc:

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

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 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 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

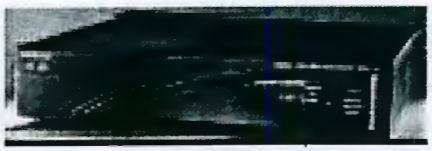
For Cisco IOS Images containing firewall (FW) and intrusion detection (IDS) capabilities, see individual product pages of supported platforms and the Cisco IOS Feature Navigator at http://www.cisco.com/go/fn (CCO login required) for part numbers and more info.

For More Information

See the Cisco IOS Firewall Feature Set Web site: **http://www.cisco.com/go/csis**

ECT 3645
RQS Nº 03/2005 - CN
PMI - CORREIOS
Fls: 0578
Doc: 3701

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-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

ECT 3643
RQS Nº 03/2005 - CN
CPMI - CORREIOS
0579
Fls:
Doc: 3701

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).

ECT 3641

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)

ROS Nº 03/2005 - CN
CPMI - CORREIOS
0580
Fls:
Doc: 3701

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

ECT 3639

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 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 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

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0581
Fls:
Doc: 3701

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
- Nokia: IP440
- Nortel: Contivity 4500

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 Service's 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

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0582
Fls:
Doc:

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

ECT 3635 21

- 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.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0583
Fls: 3701
Doc:

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

RQS 005 - CN
CPI RREIOS
3701
0584
Doc:

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
- Network Appliance: NetCache C1200/2100/6100 Series Appliances and Content Director
- Volera: Excelerator, Media Excelerator, Secure Excelerator

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)

RQS-Nº 03/2005 - CN
CPMI - CORREIOS
0585
Fls:
Doc: 3701

Selected Part Numbers and Ordering Information[1]

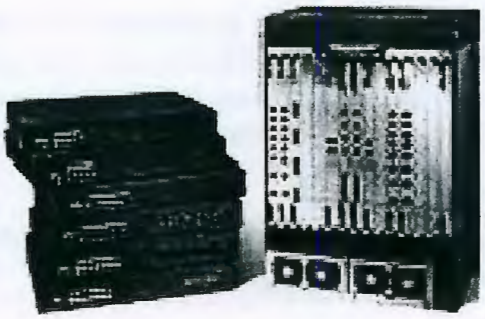
Cisco Content Engine 7300 Series Hardware	
CE-7325-K9	Content Engine 7325 AC Power, ACNSsoftware
CE-7305-K9	Content Engine 7305 AC Power, ACNS software. Also runs as CDM or CR
Cisco Content Engine 500 Series Hardware	
CE-565-K9	Cisco Content Engine 565, AC Power, ACNS software. Also runs as CDM or CR
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 numbe and pricing info, see the *Distribution Product Reference Guide* at: http://www.cisco.com/dprg (limited country availability)

ECT 3629
ROS Nº 03/2005 - CN
CPMI - CORREIOS
0586
6-5
Fls:
3701
Doc:

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 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

ECT 3627

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.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0587
Fls: 3701
Doc:

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.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0588
6-9
Fls:
3701
Doc:

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

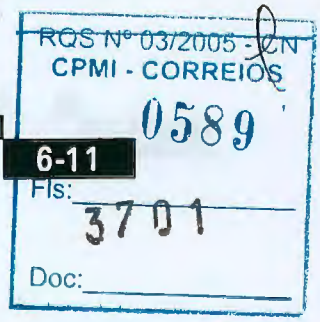
Selected Part Numbers and Ordering Information[1]

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.

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**

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0590
Fls:
Doc: 3701

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**

ECT 3618 20
RQS Nº 03/2003 - CN
CPMI - CORREIOS
0591
Fls:
Doc 3701

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

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0592
3701
Doc:

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.

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

ECT 362 CPMI-AC

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0594
Fls: 7-5
Doc: 3701

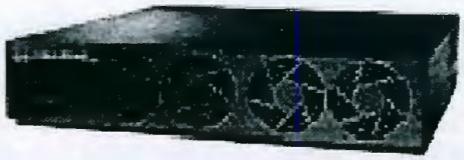
Cisco AS5350 Software	
S535AK8-12202XA	Cisco AS5350 Series IOS ENTERPRISE PLUS IPSEC 56
S535AP-12202XA	Cisco AS5350 Series IOS ENTERPRISE PLUS
S535CK8-12202XA	Cisco AS5350 Series IOS IP PLUS IPSEC 56
S535CP-12202XA	Cisco AS5350 Series IOS IP PLUS
Cisco AS5350 Memory Options & Spares	
MEM-UP1-AS535	16M 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.

C T 360 C P L - A S

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
- 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) 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

BOS-N° 03/2005 - CN - CPMI - CORREIOS 0595 Fls: 3701 Doc:

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**

ECT 3608

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

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 0596
Doc: 3791

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**

ECT 3606 21
RQS Nº 03/2005 - CN
CPMI - CORREIOS
0597
Fls:
3701
Doc:

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.

ECT 3604

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.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0598
Fls:
Doc: 3707

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

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

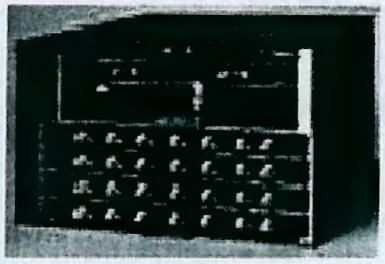
Feature	Cisco uBR7111 and uBR7114	Cisco uBR7111E and uBR7114E
Memory	Flash: 48 MB; System: 128 MB	Flash: 48 MB; System: 128 MB
Line Card with Integrated Upconverter (Cable Plant Interface)	uBR7111: 1 downstream and 1 upstream uBR7114: 2 downstream and 4 upstreams	uBR7111E: 1 downstream and 1 upstream 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

ECT 3602
ROS Nº 03/2005 - CN
CPMI - CORREIOS
0599
Fls:
Doc: 3701

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: 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.

ECT 3600
PROCESSO 03/2005 - CN
CPMI - CORREIOS
0600
Fls:
Doc: 3701

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

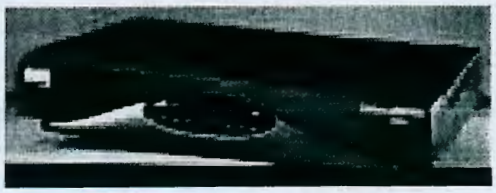
Feature	Cisco RF Switch
Environmental	• Operational temperature range: 0 to +40°C • Operating temperature range: -5 to +55°C
RF requirements	• Input/output impedance: 75 ohms • Maximum RF input power: +15 dBm (63.75 dBmV) • Switch type: Electro-mechanical, absorptive for working path, non-absorptive 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

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 Cisco uBR925 Cable Access Router	• Data-only broadband services (or voice separately via Ethernet) • High-speed, secure remote tunneling via hardware accelerated IPSec VPN • 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.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0601
Fls:
Doc: 3701

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.

3596

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

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0602
Fls:
Doc: 3701

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.

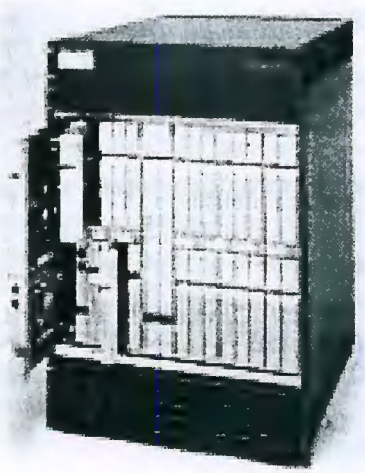
The Cisco BPX 8600 series switch offers up to 20 Gbps of high-throughput switching for multiple traffic types data, voice, and video and supports a wide range of interfaces, from Frame Relay to full broadband subscriber interfaces, up to 622 Mbps. You can offer multiple services for LAN, X.25, SNA, IP, 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**

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0603
Fls:
Doc: 3701

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**

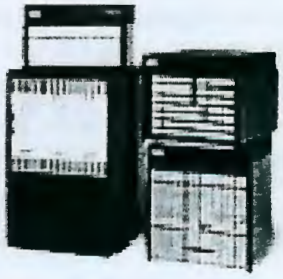
Cisco MGX 8830 ATM Multiservice Switch

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.

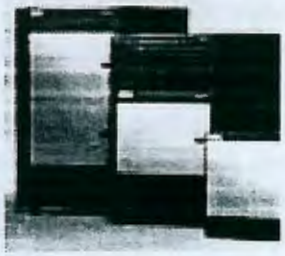
Cisco MGX 8250 Edge Concentrator

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.

ECT 3502
ROS Nº 03/2005 - CN
CPMI - CORREIOS
0604
Fls:
Doc: 3701

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

REQ Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 0605
Doc: 3791

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

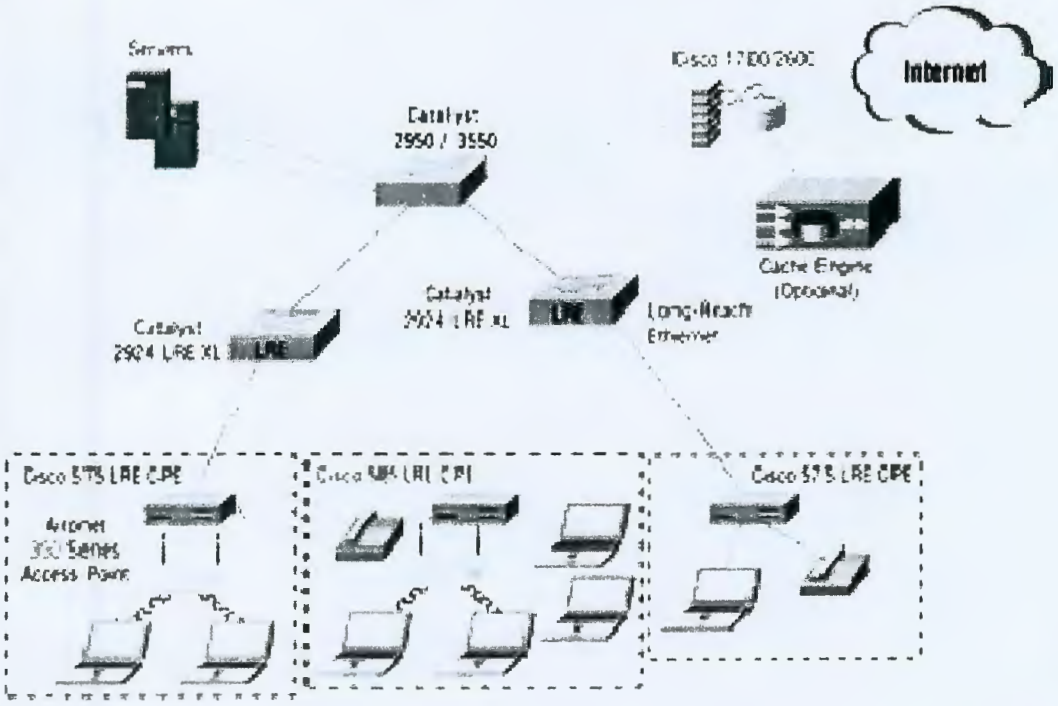
The Cisco Building Broadband Service Manager (BBSM) Hotspot server connects mobile users to broadband services anywhere, anytime. Cisco BBSM Hotspot is a cost effective access management gateway suited for small- to medium-sized public access locations, as well as for visitor access in larger enterprise 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



RQS Nº 03/2005 - CN
CPMI - CORREIOS
0606
Fls:
Doc:

CHAPTER 8

Optical Transport

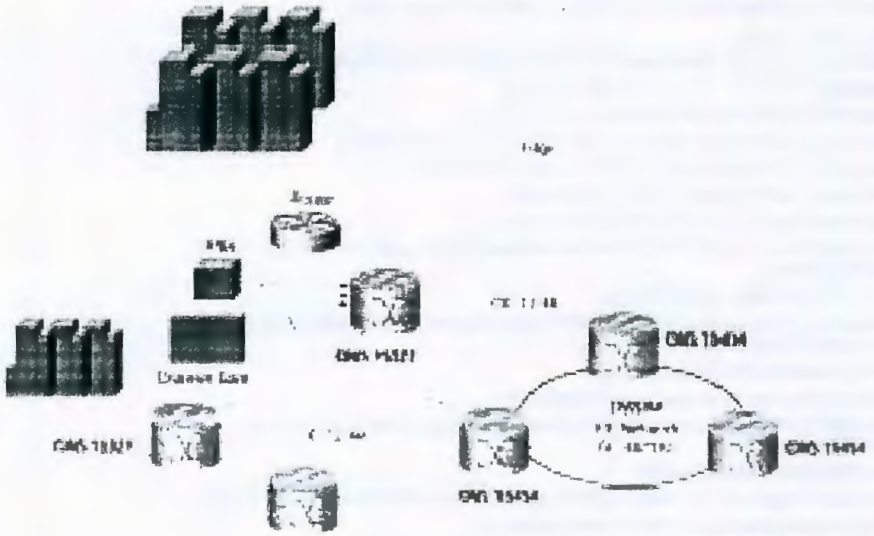
Optical Transport Products at a Glance

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

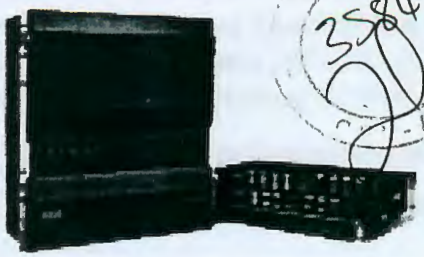
RQS Nº 03/2005 - CP
CPMI - CORREIOS
0607
Fls:
Doc: 3701

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

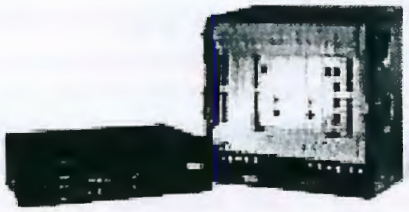
EQS Nº 03/2005 - CN - CPMI - CORREIOS
0608
Doc: 3701

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**

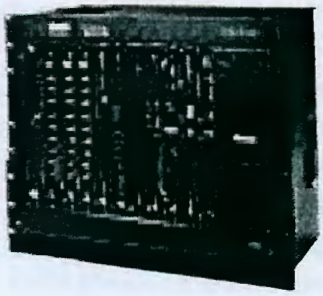
Cisco ONS 15501 Erbium Doped Fiber Amplifier

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

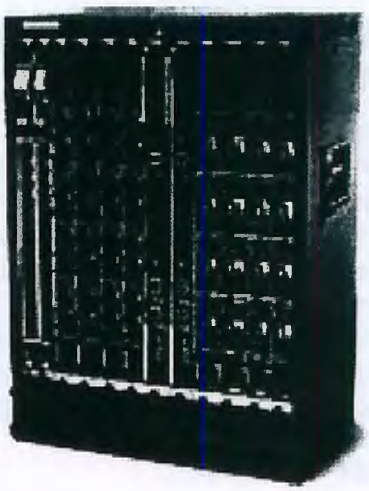
- Aggregation—up to 40 ports of ESCON or 8 ports of Fibre Channel, FICON, or Gigabit Ethernet per wavelength, lowering total cost of ownership through bandwidth efficiency
- Scalability—up to 32 wavelengths ranging from 2.5Gbps to 10Gbps for network growth and design flexibility
- Multiservice Interfaces—protocol-independent 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**

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0609
Fls:
3701
Doc:

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

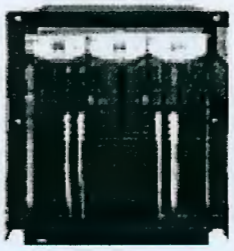
Key Features:

- 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



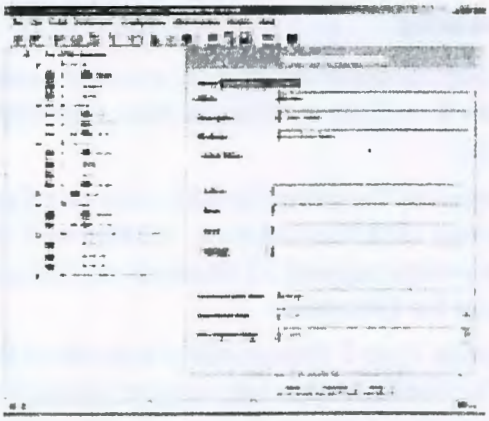
The Cisco ONS 15600 provides unparalleled flexibility in designing next generation metro networks. Fully engineered and optimized for metro networks, the Cisco ONS 15600 MSSP simplifies and revolutionizes bandwidth management in the metro core by allowing service providers to seamlessly integrate their 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**

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 0610
Doc: 3701

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.

CHAPTER 9

IOS Software & Network Management

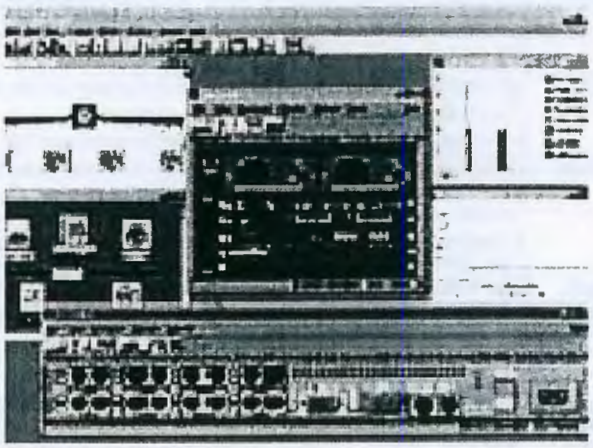
Cisco IOS® Software & Network Management Products at a Glance

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

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0611
Fls:
Doc: 3701

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

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0612
Fls:
Doc:

3701

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

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0613
Fls:
3701
Doc:

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**

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0614
Fls: 3701
Doc:

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**

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 0615
3701
Doc:

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

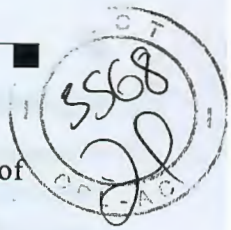
There are three categories of Cisco IOS Software releases: Early Deployment, Major, and General Deployment (GD) releases.

- 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.

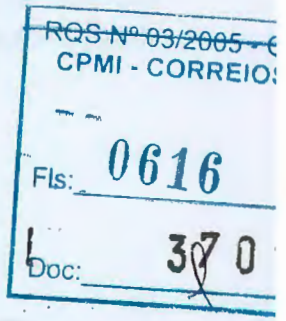
CiscoWorks Small Network Management Solution

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

ECT
RQS Nº 03/2005 - CN
CPMI - CORREIOS
0617
Fls:
Doc: 3701

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.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0618
Fls:
3701
Doc:

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

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0619
Fls:
3701
Doc:

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

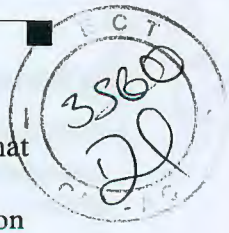
Optional Drop-In Modules

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 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

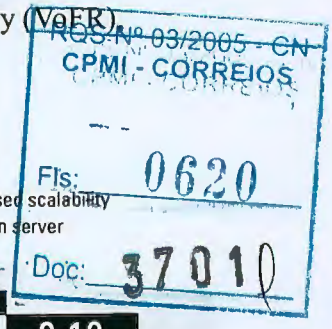
CWITEM-1.3-WIN-K9	CiscoWorks IP Telephony Environment Manager 1.3 for Windows Add-On for existing LMS 2.X and DFM 1.1 customers; includes VHM only
CWITEM-1.3-WIN-UP	CiscoWorks VoIP Health Monitor 1.0 Add-On for existing LMS 2.0 and DFM 1.1 customers; includes VHM only
CWITEM-1.3-MR-K9	Maintenance kit 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

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]

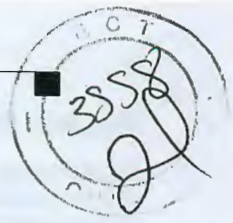
CiscoWorks Voice Manager for Voice Gateways 2.1 9

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

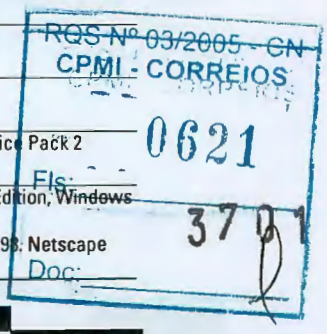
Sell This Product	When a Customer Needs These Features
Cisco QoS Policy Manager	• End-to-end QoS configuration and automated, reliable policy deployment, while eliminating device-by-device command streams • Rules-based policies that combine static and dynamic port applications and host system traffic 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

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0622
Fls:
3701
Doc:

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**

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0623
Fls:
Doc: 3701

AP BG

RQS Nº 03/2005 - CN
CPMI - CORREIOS

Fls: 3701
0624
Doc:

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 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

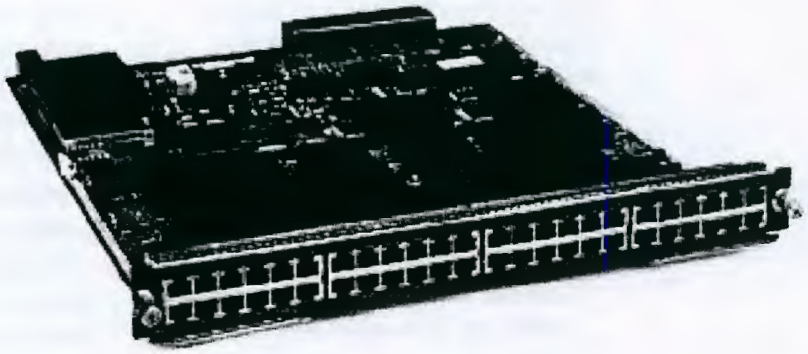
Cisco Systems, Inc.
All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS Nº 03/2005 - CPMI - CORREIOS
0625
Fls: 3701
Doc:

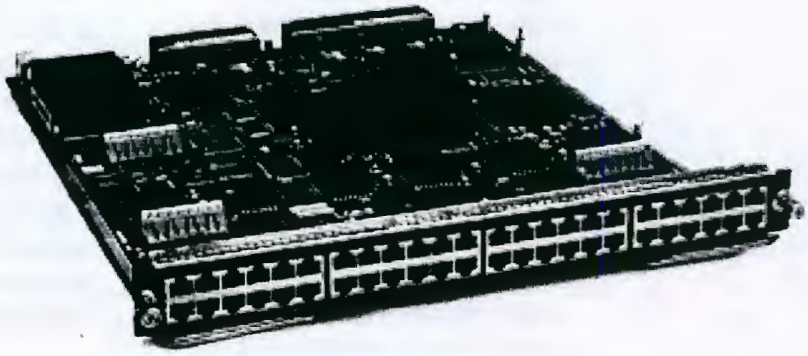
- Operational consistency—Supported in all Catalyst 6500 3-, 6-, 9-, and 13-slot chassis running Cisco IOS® Software and Cisco Catalyst Operating System Software; interoperable with all other interfaces and services modules; and forward-compatible with all Catalyst 6500 supervisor engines
- Maximum network 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 network 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 Systems, Inc.
All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

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

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

ECT 3550 21

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0626
Fls: 3701
Doc:

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 Systems, Inc.
All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

ECT 3548 CPMI - CORREIOS

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.

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0627
Fls:
Doc: 3701

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

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

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

Cisco Systems, Inc.
All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

ROS Nº 03/2005 - CN
CPMI - CORREIOS
0628
Fls:
3701
Doc:

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

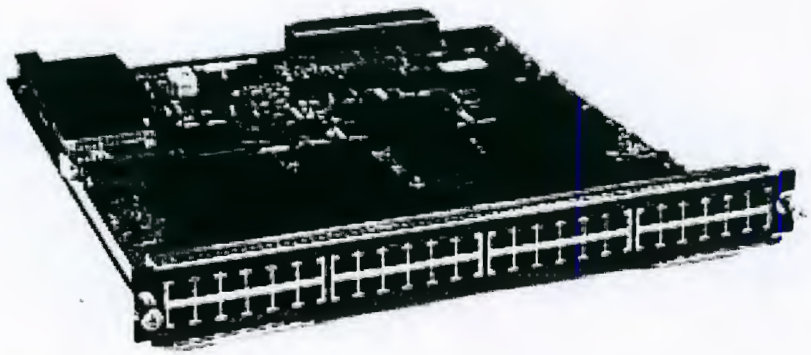
Transmit queue structure—1p2q2t = 1 strict priority queue, 2 round robin queues, 2 thresholds

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



All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

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

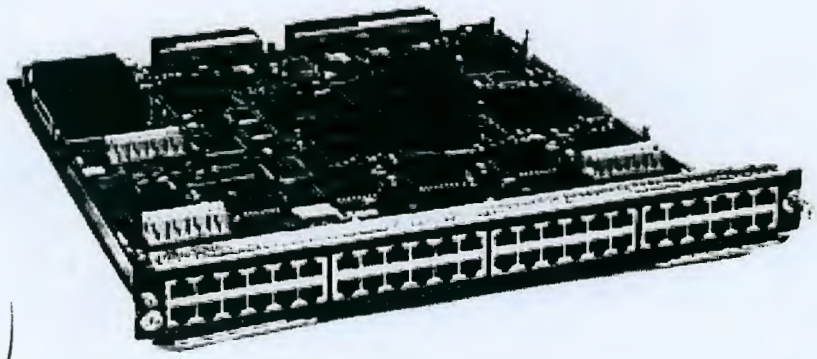
Transmit queue structure—1p2q2t = 1 priority queue, 2 round robin queues, 1 threshold

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



All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0629
Fls:
Doc:
3701

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

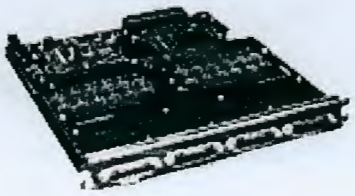
Receive queue structure—1q4t = one round robin queue and four thresholds

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

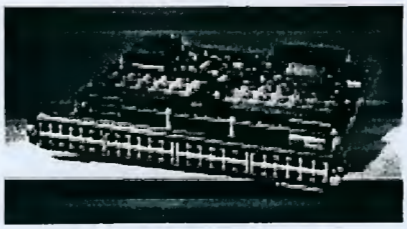
Table 7 Classic 10/100 Copper Voice Interface Modules

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



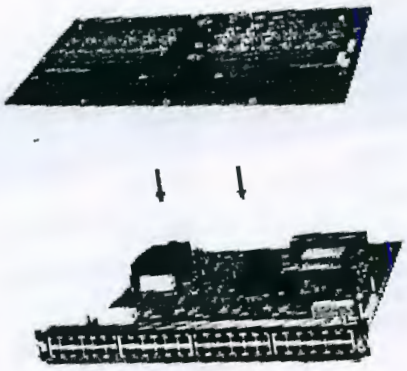
VWS-X6148-RJ21V



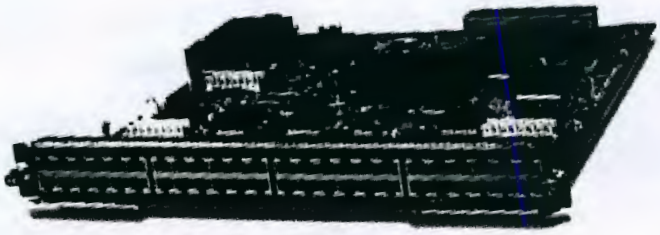
All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 0630
Doc: 3701

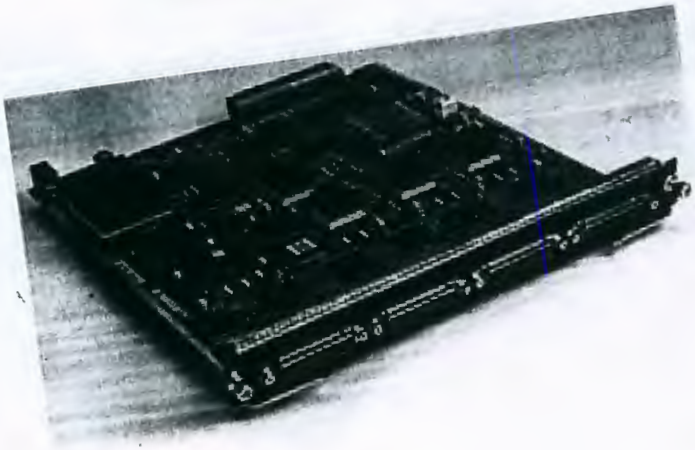
WS-X6348-RJ21V



WS-X6148-RJ-45



WS-X6148-RJ-21



Cisco Systems, Inc.
All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

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

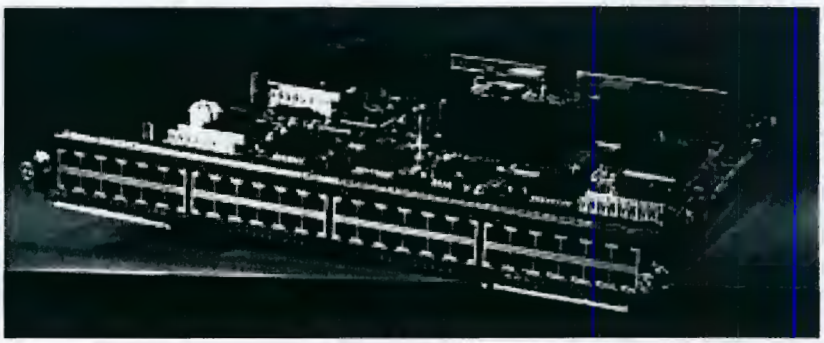
Product	Ports/Interface/ Connectors	Port Density/Chassis Model	Maximum Distance/ Cable Type
WS-X6548-RJ-45	48-port; 10/100BASE-TX; RJ-45	576 ports (Cisco Catalyst 6513); 384 ports (Cisco Catalyst 6509)	100 meters; Category 5 cable
WS-X6548-RJ-21	48-port; 10/100BASE-TX; RJ-21	576 ports (Cisco Catalyst 6513); 384 ports (Cisco Catalyst 6509)	100 meters; Category 5 cable

Cisco Systems, Inc.
All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

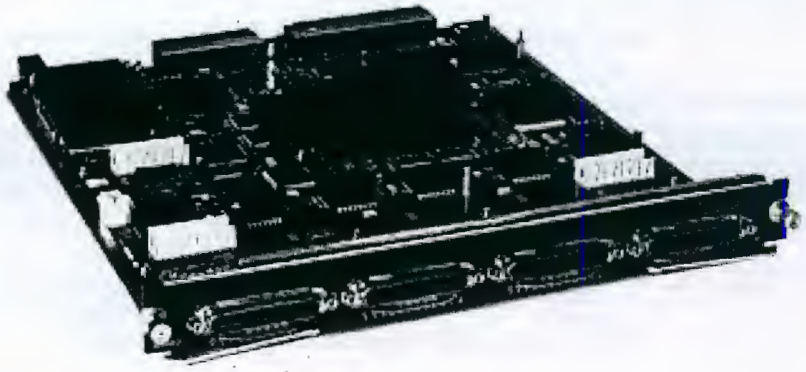
RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 0631
Doc: 3701

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



All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

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

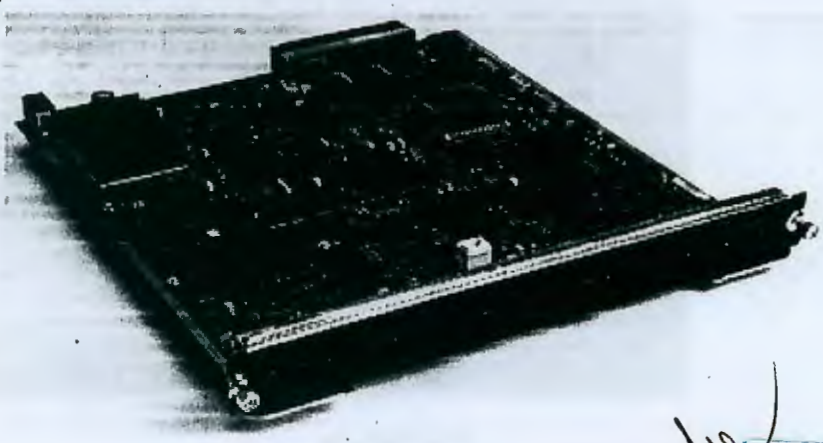
Receive queue structure—1q4t = 1 round robin queue, 4 thresholds

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 Systems, Inc.
All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0632
Fls:
3701
Doc:

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 Engine 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

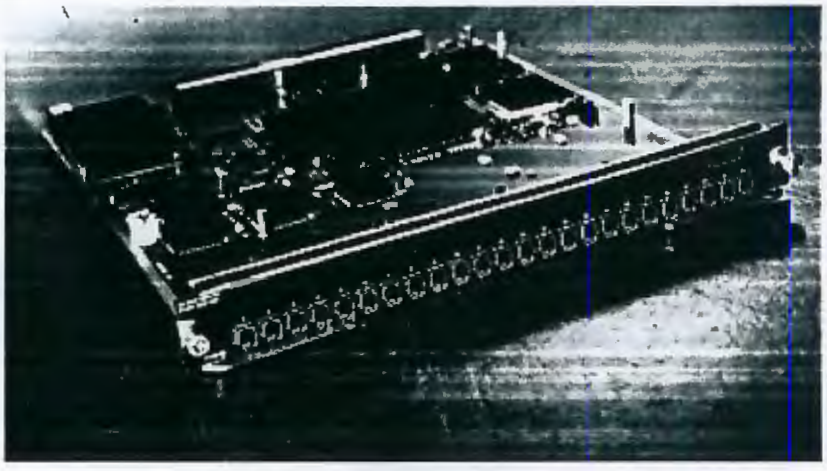
Receive queue structure—1p1q2t = 1 priority queue, 1 round robin queue, 2 thresholds

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



Cisco Systems, Inc.
All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

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

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS Nº 03/2005 - CN
GPMI - CORREIOS
0633
Fls: 3701
Doc:

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

Cisco Systems, Inc.
All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

- 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

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0634
Fls:
3701
Doc:

- 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:

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

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

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

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Catalyst, Cisco, Cisco IOS, Cisco Systems, the Cisco Systems logo, EtherChannel, and SMARTnet are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0304R)

ECT 3532 C - AG

ECT - 03/2005 - SN
CPMI - CORREIOS
MH/LW4273 0403
Fls: 0635
Doc: 3701

Ap Bfl

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 0636
Doc: 3701

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

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 3701
Doc:

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:

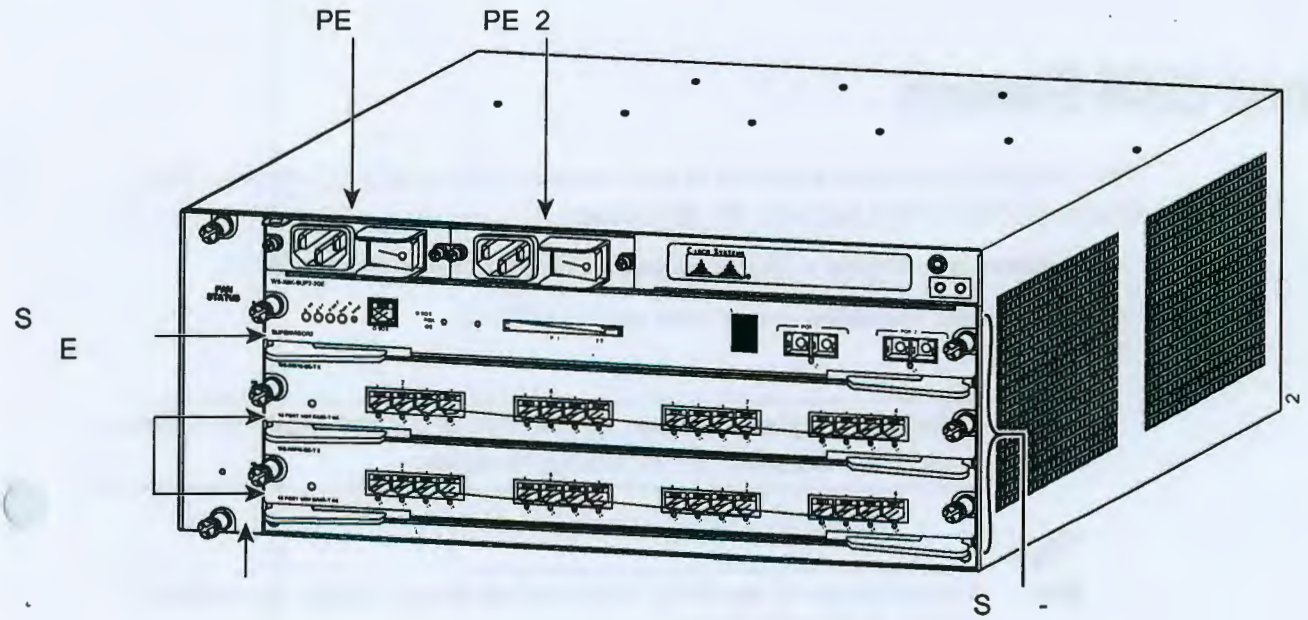
- A supervisor engine with two gigabit interface uplinks and an optional redundant supervisor engine in one of the following configurations:
  - Two supervisor engines, each with no Multilayer Switch Feature Card (MSFC) and no Policy Feature Card (PFC)
  - Two supervisor engines, each configured with 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.

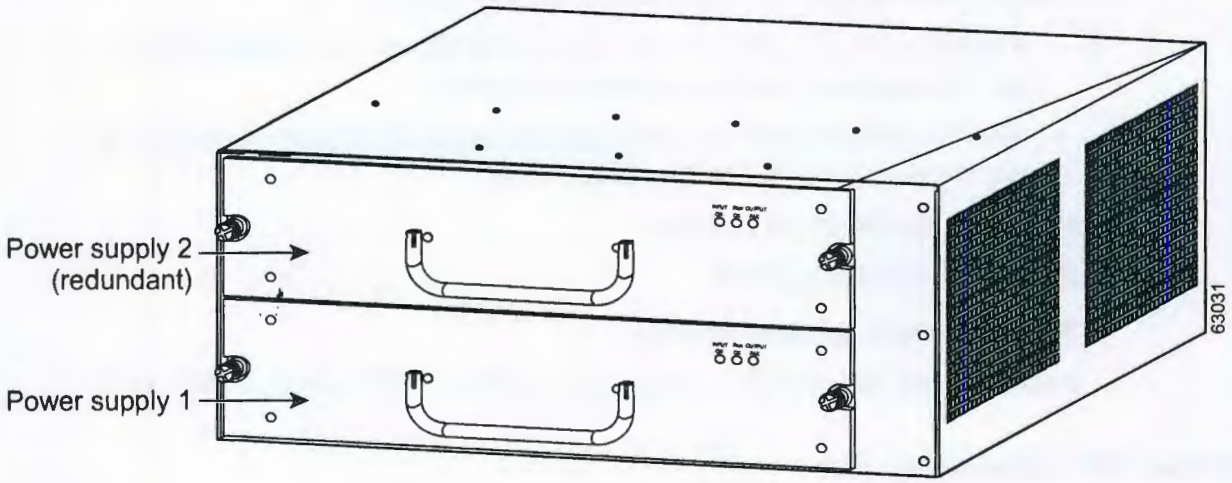
- Up to two hot-swappable Catalyst 6500 series modules:
  - The Switch Fabric Modules (WS-C6500-SFM and WS-X6500-SFM2) are not supported on the Catalyst 6503 switch.
  - The WS-X6816-GBIC 16-port Gigabit Ethernet fabric-enabled module is not supported on the Catalyst 6503 switch.
- Backplane bandwidth 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



RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 0638
Doc: 3701

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

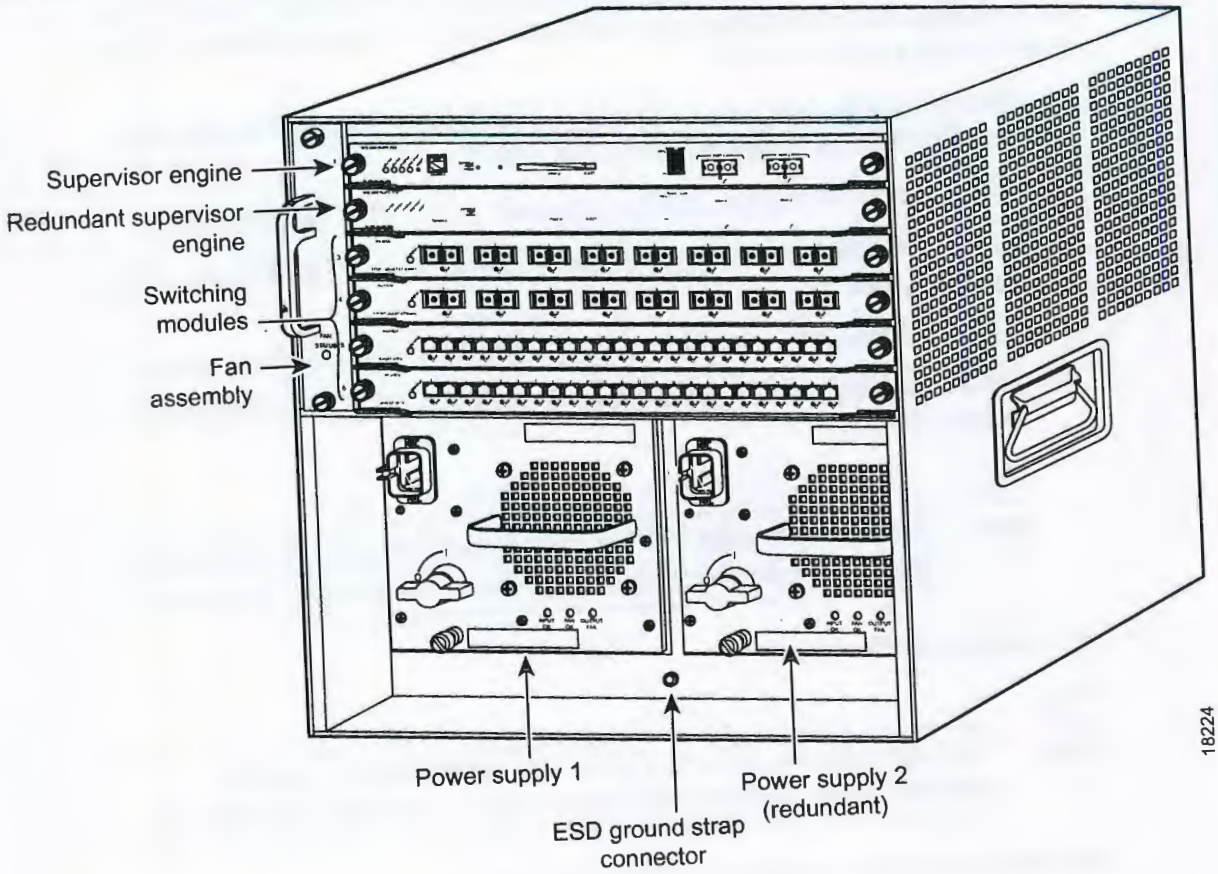
Note When a Supervisor Engine 720 and the high capacity fan tray are installed, you must install 2500 W or higher capacity power supplies in the chassis.

- 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.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 3701
Doc:

Figure 1-3 Catalyst 6506 Switch



- 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.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0640
Fls:
3701
Doc:

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.

3523
CPMI - CO

  - 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

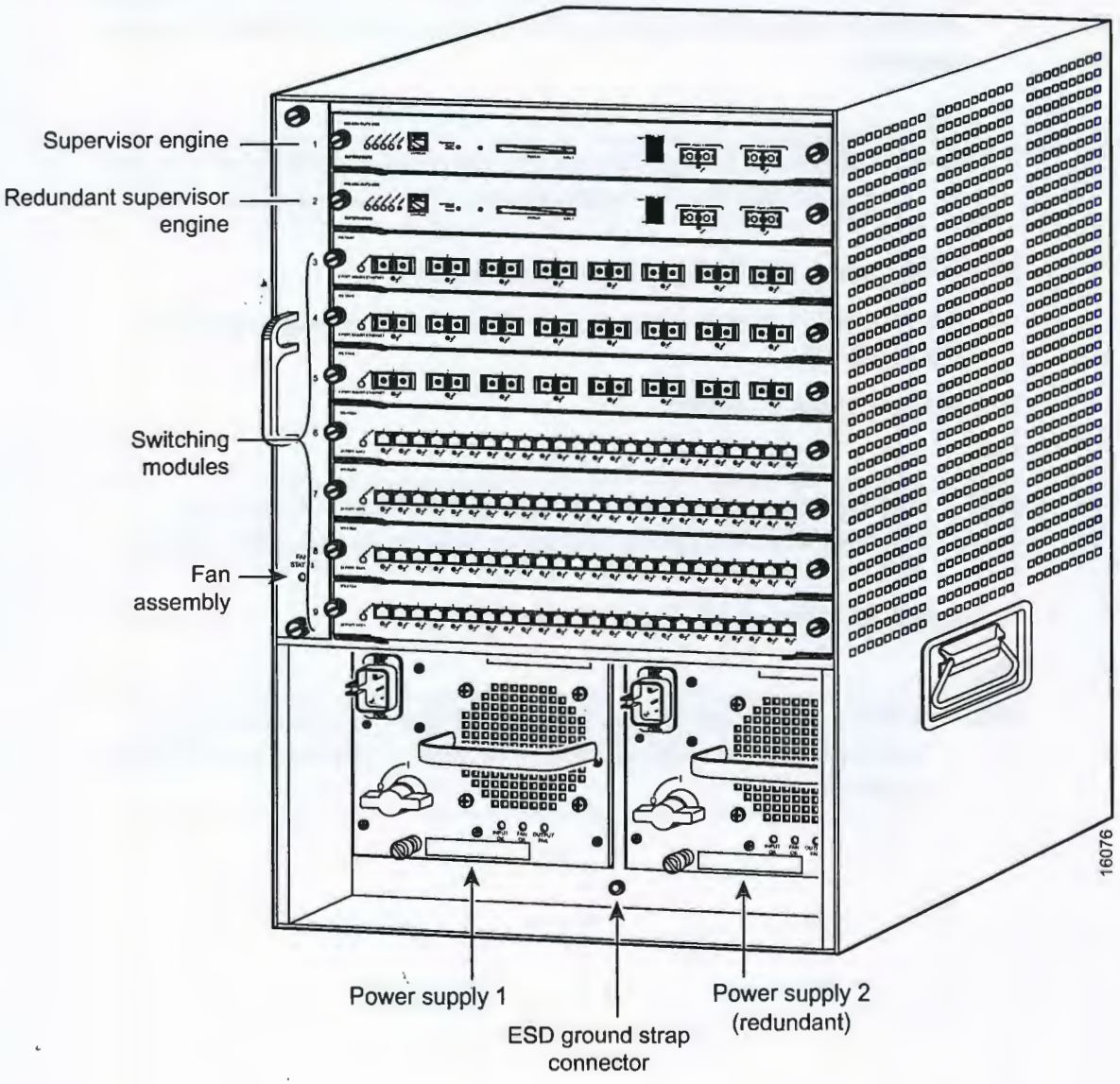
Note The high capacity fan tray (WS-C6K-9SLOT-FAN2) must be installed when a Supervisor Engine 720 is installed in the chassis.

- 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.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0641
Fls:
Doc: 3701

Figure 1-4 Catalyst 6509 Switch



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

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1-11
Fls:
Doc: 3701

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.

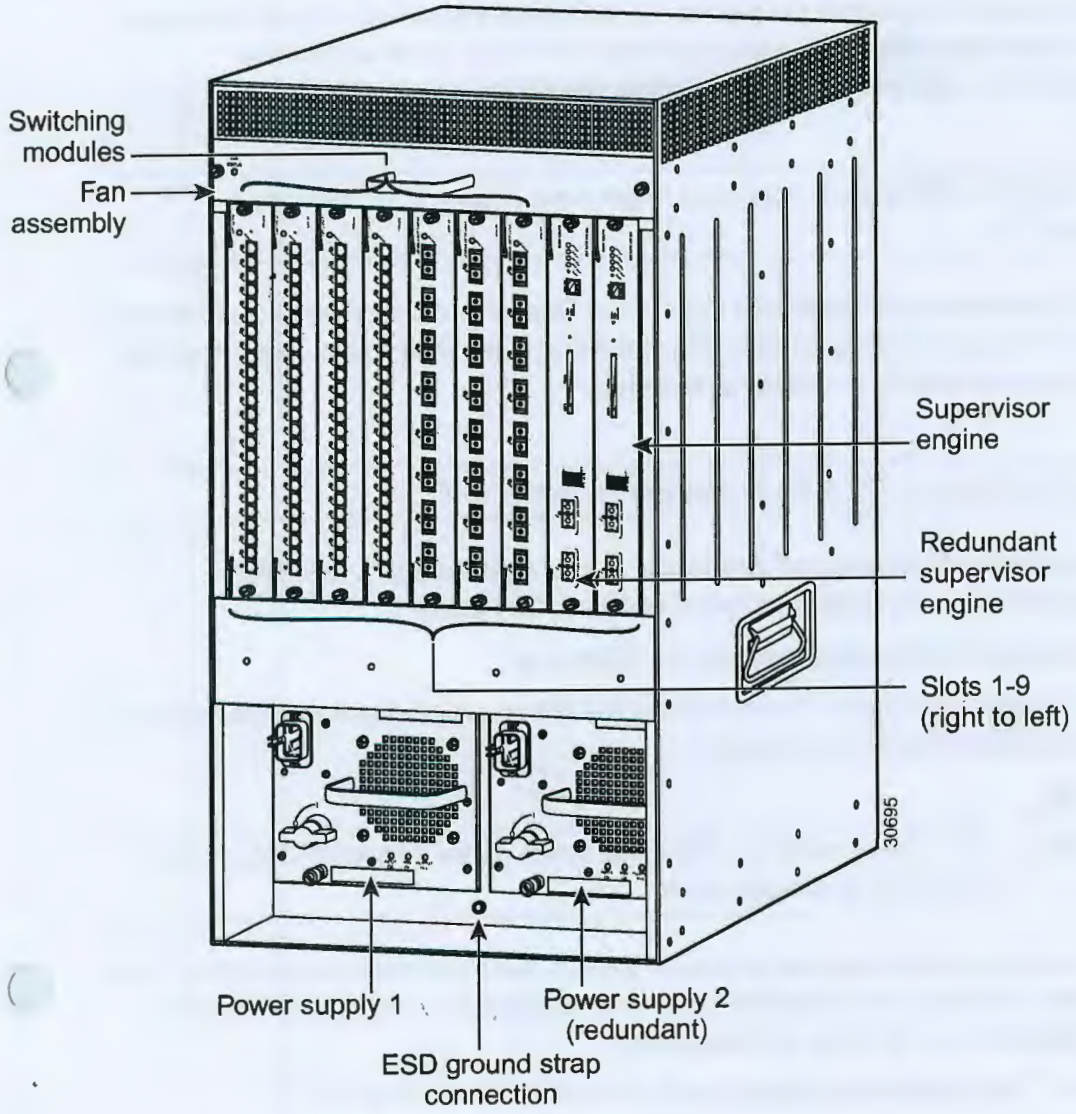
- Up to eight additional Catalyst 6500 series hot-swappable modules
  - Fabric-enabled module support provided in all slots (requires Switch Fabric Module or Supervisor Engine 720)
- Hot-swappable fan assembly

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



RQS Nº 03/2005 - CN
CPMI - CORREIOS
1-13
0643
Fls:
3791
Doc:

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

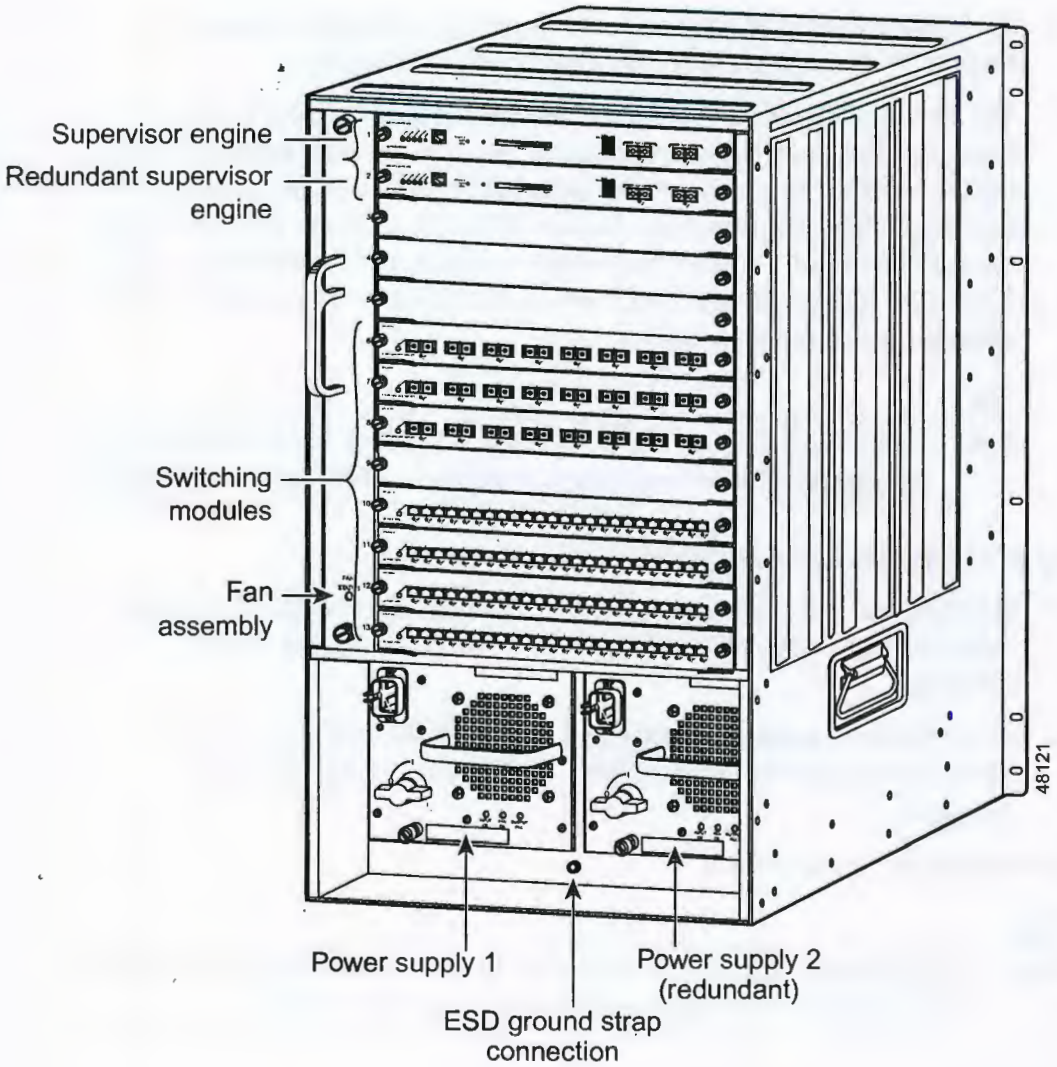
Note The high capacity fan tray (WS-C6K-13SLT-FAN2) must be installed when a Supervisor Engine 720 is installed in the chassis.

- Redundant AC-input or DC-input power supplies

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 0644
Doc: 3701

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



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

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1-17
0045
Fls:
3701
Doc:

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

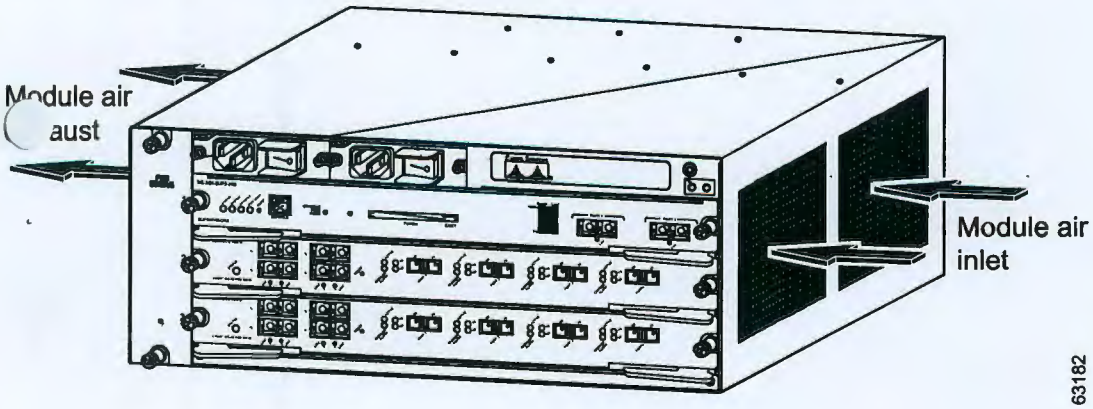


Figure 1-8 Catalyst 6506 Switch Internal Airflow

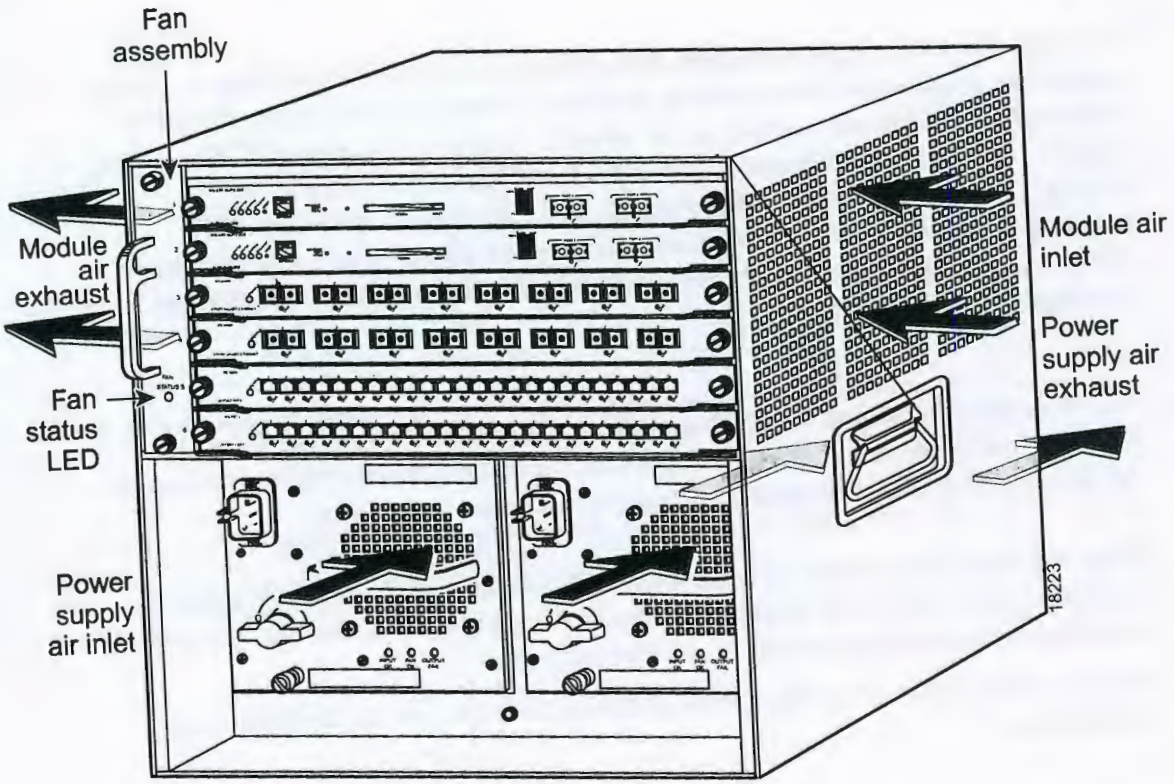
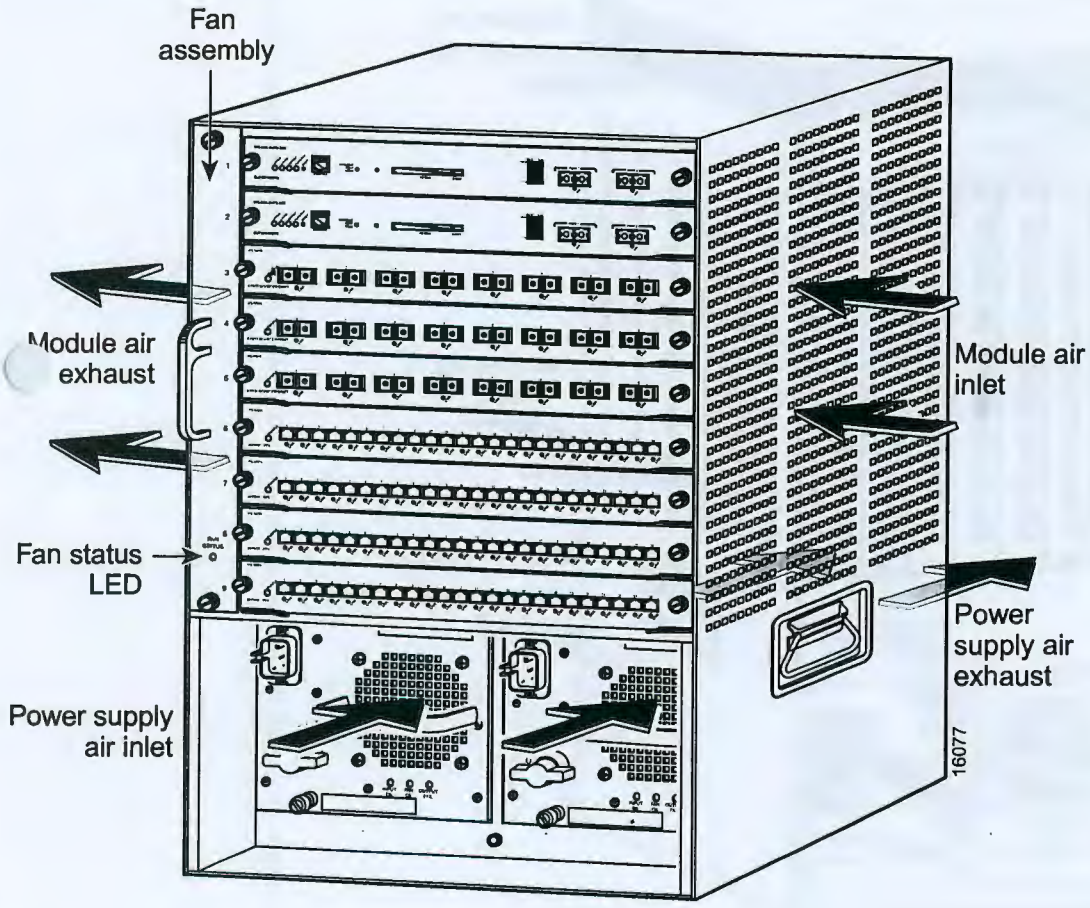


Figure 1-9 Catalyst 6509 Switch Internal Airflow



RQS Nº 03/2005 - CN - CORREIOS
1-21
Fls: 0647
Doc: 3701

Figure 1-10 Catalyst 6509-NEB Switch Internal Airflow

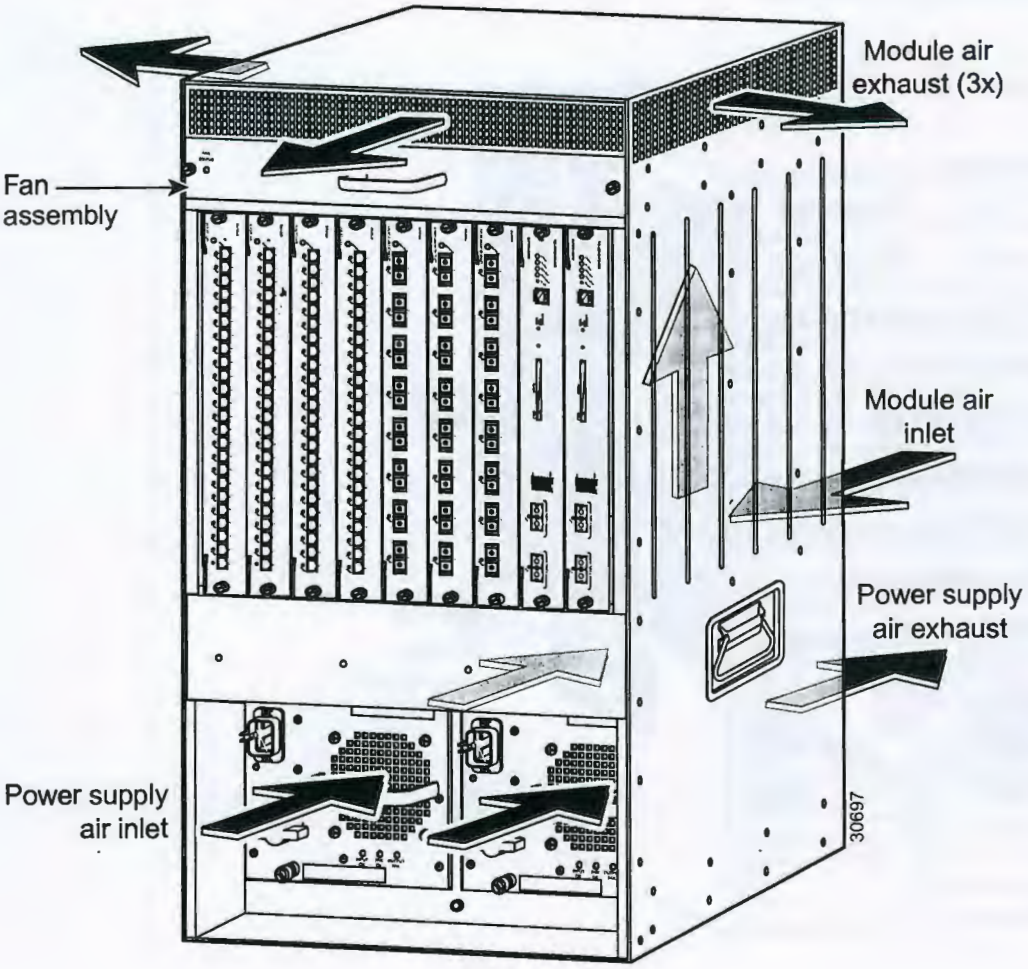
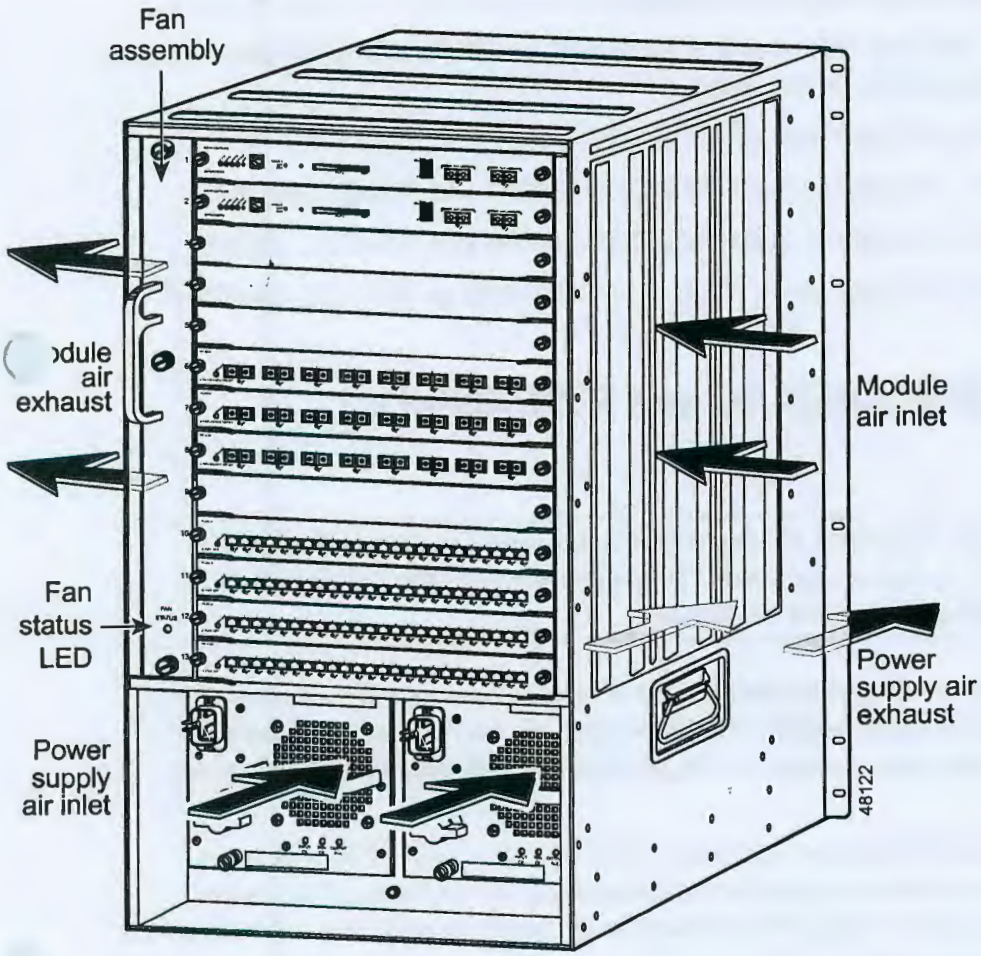


Figure 1-11 Catalyst 6513 Switch Internal Airflow



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

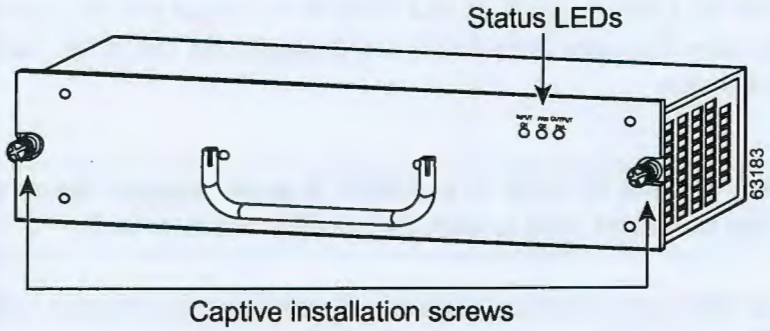


Figure 1-13 Catalyst 6503 AC Power Entry Module (PEM)

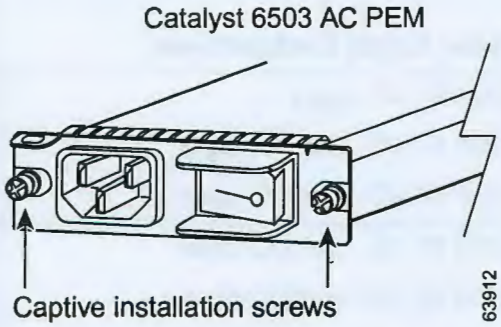
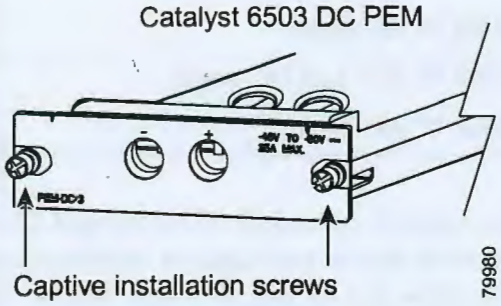


Figure 1-14 Catalyst 6503 DC Power Entry Module (PEM)



RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 0649
3701
Doc:

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."

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0650
Fls: 3701
Doc:

Figure 1-15 AC-Input Power Supply

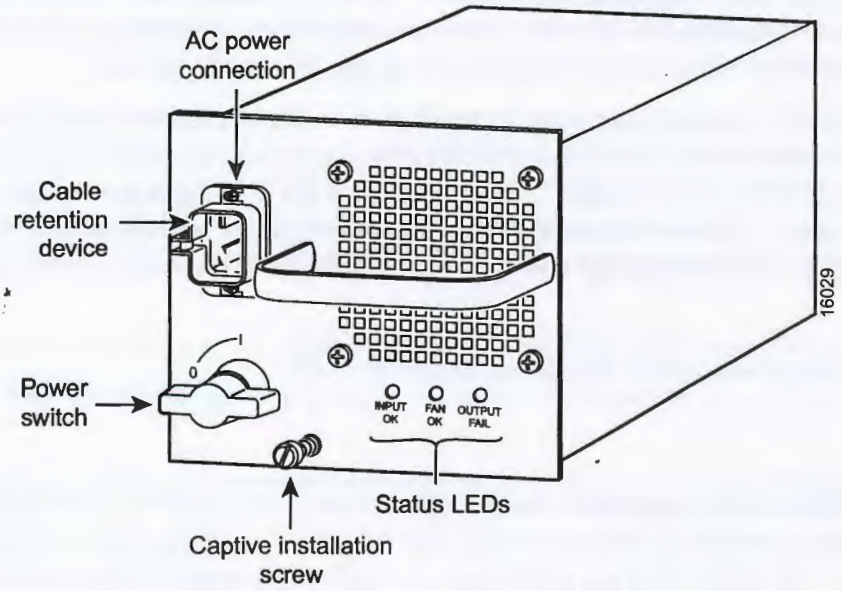
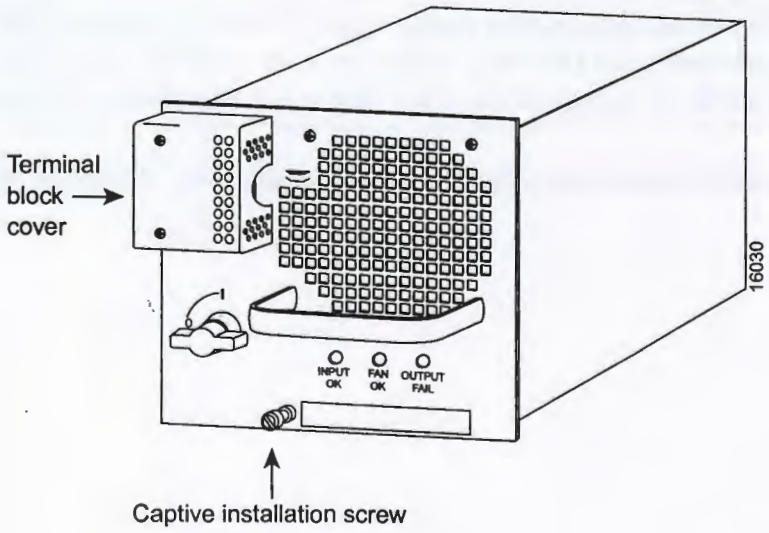


Figure 1-16 DC-Input Power Supply



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.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 0651
Doc: 3701

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.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 0652
Doc: 3701

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.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 0653
Doc: 3701

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.

AP B1

RQS Nº 03/2005 - CN
CPMI - CORREIOS

Fls: 0654

Doc: 3701

Cisco Catalyst Operating System Software Version 7.1(1) for the Catalyst 6000 and 4000 Series Switches

The Cisco Catalyst Operating System software Version 7.1(1) for the Supervisor Engine supports the Cisco Catalyst 6000 and Catalyst 4000 Series switches.

Hardware Supported

The system software version 7.1(1) supports all cards already previously supported by the Cisco Catalyst Operating System software on the Cisco Catalyst 6000 and Cisco Catalyst 4000 Series Supervisor Engines. In addition, the Catalyst Operating System software release 7.1.1 supports the following additional hardware modules:

Hardware Module	Description	Catalyst 6500 Module	Catalyst 4000 Module
WS-X6501-10GEX4	1-port 10-Gigabit Ethernet Module	X	
WS-X6524-100FX-MM	24-port 100BaseFX Ethernet Module	X	
WS-X4448-GB-RJ45	Catalsyt 4000 Family 48-port 10/100/1000 BASE-T Module		X

The Catalyst Operating System software release 7.1.1 also includes support for the Cisco 7603 Internet Router:

Hardware	Description
Cisco7603	Cisco 7603, 3-slot Chassis

Note: The Cisco 7603 Internet Router supports all Supervisor Engine configurations.

ROS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 0655
Doc: 3701

All contents are Copyright © 1992--2001 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Software Features

The following software features all require Cisco Catalyst Operating System system software 7.1(1) for the Supervisor Engines.

Software Feature	Description	Catalyst 6000 Feature	Catalyst 4000 Feature
IEEE 802.3ad	Link Aggregation Control Protocol, (LACP) is defined in IEEE 802.3ad and allows Cisco switches to manage Ethernet channeling with devices that conform to the 802.3ad specification. LACP is similar to Cisco's proprietary implementation of EtherChannel, Port Aggregation Protocol (PAgP) which allows ports with similar characteristics to form a channel through dynamic negotiation with a partner system.	X	X
EE 802.1w/802.1s	The IEEE 802.1w specification, (Rapid Spanning Tree Protocol) provides for sub-second reconvergence of the Spanning Tree Protocol after failure of one of the uplinks in a bridged environment. 802.1w provides the structure on which the 802.1s feature operates. The IEEE 802.1s specification (MST - multiple Spanning Tree) allows a user to build multiple spanning trees over VLAN trunks. Fast convergence of the MST topology is achieved by using a modified version of the RSTP protocool.	X	X
BPDU Filtering Per Port	With Version 7.1(1) of the Catalyst Operating system, BPDU Filtering can now be applied on a per-port basis. BPDU Filtering (both ingress and egress) can now be enabled on any ports, including non-portfast-enabled and trunk ports.	X	
IGMP Snooping on Private VLANs	IGMP Snooping can be applied on a Private VLAN.	X	
IGMP Snooping Querier	This feature provides the ability to run IGMP Snooping in the absence of a multicast router. The switch then acts as an IGMP Querier.	X	
MP Filtering	IGMP Filtering enables the Catalyst 4000 to filter (permit or deny) IGMP packets by allowing the configuration of profiles of IP multicast groups. A profile consists of one or more ranges of IP multicast addresses which can then be filtered or monitored on a per switch port basis. The monitoring function of IGMP filtering enables administrators to track the time and duration that a port has been a member of an IP multicast group.		X
Option for No VTP	Enables a switch to not only be a non-participant in VTP, but also to drop all VTP traffic (unlike Transparent mode which passes VTP traffic) thus creating a VTP boundary.	X	X

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0656
Fls:
Doc: 5791

All contents are Copyright © 1992--2001 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Software Feature	Description	Catalyst 6000 Feature	Catalyst 4000 Feature
Portfast on Trunks	Allows portfast to be configured for trunk/channel ports. On link-up state, the port immediately transitions into Spanning Tree forwarding mode, bypassing listening and learning states. This feature is useful for direct connections to routers or servers.	X	X
Show Port MAC Address	Enables users to view the MAC address for each physical port on the switch from the switch's range of MAC addresses.	X	
Single Device Per Port Enhancement	Enables users to move hosts to different switch ports without the 10 minutes delay duration previously required by the port security feature implementation. The timer values can be set from a 1-minute minimum to 1440 minutes maximum.	X	
SMON-MIB VLAN Stats Support	Per-VLAN statistics (total packets, octets, nucast packets and nucast octets) are provided through the SMON VlanIdStatsTable of the SMON-MIB with Supervisor Engine 2 / MSFC2.	X	
MAC Address Notification	MAC Address Notification allows the network administrator to monitor the MAC addresses that are learned by the switch and those which are aged out or removed from the CAM table. Notifications can be sent to the administrator for both unicast and multicast addresses and include SNMPv2 traps or a history log of the change.		X
Various MIB Support	• CISCO-CATOS-ACL-QOS-MIB Enhancement	X	
	• CISCO-ENTITY-FRU-CONTROL-MIB Enhancement	X	X
	• CISCO-ENVMON-MIB	X	X
	• CISCO-IGMP-FILTER-MIB		X
	• CISCO-LAG-MIB	X	X
	• CISCO-MAC-NITIFICATION-MIB		X
	• CISCO-MEMORY-POOL-MIB Enhancement	X	
	• CISCO-PAE-MIB	X	X
	• CISCO-STP-EXTENSIONS-MIB	X	X
	• CISCO-SWITCH-ENGINE-MIB Enhancement	X	
	• IEEE8021-PAE-MIB	X	X
	• IEEE8023-LAG-MIB	X	X

Orderable Software Images

The following table lists the software versions and applicable ordering information for the Cisco Catalyst 6000 and Catalyst 4000 Series Supervisor Engine software. **Starting with version 7.1(1), The 'non-krypto' images will now be designated as K8 images, denoting weak encryption, where SNMPv3 and Kerberos telnet session data is encrypted.**

Caution: Always back up the switch configuration file before upgrading or downgrading the switch software to avoid losing all or part of the configuration stored in NVRAM. When downgrading switch software, you will lose your configuration. Use the **write network** command or the **copy config tftp** command to back up your configuration to a Trivial File Transfer Protocol (TFTP) server. Use the **copy config flash** command to back up the configuration to a Flash device.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 0657
Doc: 3701

All contents are Copyright © 1992--2001 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Orderable Product Number	Description	Image
SC4K-SUPK8-7.1.1	Catalyst 4K Supervisor Flash Image, Release 7.1.1	cat4000-k8
SC4K-SUPK8-7.1.1=	Spare	
SC4K-SUPK9-7.1.1	Catalyst 4K Supervisor Flash Image w/SSH, Release 7.1.1	cat4000-k9
SC4K-SUPK9-7.1.1=	Spare	
SC4K-SCVK8-7.1.1	Cat4K Cisco View, Release 7.1.1	cat4000-cv
SC4K-SCVK8-7.1.1=	Spare	
SC6K-SUPK8-7.1.1	Catalyst 6000 Supervisor 1 Flash Image, Release 7.1.1	cat6000-supk8
SC6K-SUPK8-7.1.1=	Spare	
SC6K-SUP2K8-7.1.1	Catalyst 6000 Supervisor 2 Flash Image, Release 7.1.1	cat6000-sup2k8
SC6K-SUP2K8-7.1.1=	Spare	
SC6K-SCVK8-7.1.1	Cat6K Supervisor 1 Flash Image w/CiscoView, Release 7.1.1	cat6000-supcvk8
SC6K-SCVK8-7.1.1=	Spare	
SC6K-S2CVK8-7.1.1	Cat6K Supervisor 2 Flash Image w/CiscoView, Release 7.1.1	cat6000-sup2cvk8
SC6K-S2CVK8-7.1.1=	Spare	
SC6K-SUPK9-7.1.1	Catalyst 6000 Supervisor 1 Flash Image w/SSH, Release 7.1.1	cat6000-supk9
SC6K-SUPK9-7.1.1=	Spare	
SC6K-SUP2K9-7.1.1	Catalyst 6000 Supervisor 2 Flash Image w/SSH, Release 7.1.1	cat6000-sup2k9
SC6K-SUP2K9-7.1.1=	Spare	
SC6K-SCVK9-7.1.1	Catalyst 6000 Supervisor 1Flash Image w/CiscoView & SSH, Release 7.1.1	cat6000-supcvk9
SC6K-SCVK9-7.1.1=	Spare	
SC6K-S2CVK9-7.1.1	Catalyst 6000 Supervisor 2 Flash Image w/CiscoView & SSH, Release 7.1.1	cat6000-sup2cvk9
SC6K-S2CVK9-7.1.1=	Spare	

For more detailed information, refer to the Cisco Catalyst 6000 Series release notes.

Also, review the Catalyst 6000 Series documentation at:

http://www.cisco.com/warp/public/cc/pd/si/casi/ca6000/index.shtml

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0658
Fls:
3701
Doc:

All contents are Copyright © 1992--2001 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

3493

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.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 Australia, Pty., Ltd
Level 17, 99 Walker Street
North Sydney
NSW 2059 Australia
www.cisco.com
Tel: +61 2 8448 7100
Fax: +61 2 9957 4350

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the Cisco.com 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

Copyright © 2001, Cisco Systems, Inc. All rights reserved. Catalyst, Cisco, Cisco IOS, Cisco Systems, and the Cisco Systems logo registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0108R)

Printed in the USA

CMCM 20200/2005 - CN
CPMI - CORREIOS
Fls: 0659
Doc: 3701

Ap BJ

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 0660
Doc: 3701

When you enable QoS on the switch, the port buffers are divided into one or more individual queues. Each queue has one or more drop thresholds associated with it. The combination of multiple queues within a buffer, and the drop thresholds associated with each queue, allow the switch to make intelligent decisions when experiencing congestion. Traffic sensitive to jitter and delay variance, such as VoIP packets, can be moved to the head of the queue for transmission, while other less important or less sensitive traffic can be buffered or dropped.

Port Queue and Drop Threshold Types

When QoS is enabled, the multiple queues and drop thresholds on the Ethernet module switch ports are enabled. There are several different configurations of queue types and thresholds, depending on the model of the Ethernet module.

Ingress and egress scheduling are always based on the class-of-service (CoS) value associated with the frame. By default, higher CoS values are mapped to higher queue numbers. CoS 5 traffic, typically associated with VoIP traffic, is mapped to the strict priority queue, if present.

In addition to the different queues, each standard queue has one or more drop thresholds. There are two types of drop thresholds:

- *Tail-drop thresholds*—On ports with tail-drop thresholds, frames of a given CoS value are admitted to the queue until the drop threshold associated with that CoS value is exceeded; subsequent frames of that CoS value are discarded until the threshold is no longer exceeded.

  For example, if CoS 1 is assigned to queue 1, threshold 2, and the threshold 2 watermark is 60 percent, frames with CoS 1 will not be dropped until queue 1 is 60 percent full. All subsequent CoS 1 frames are dropped until the queue is less than 60 percent full.
- *WRED-drop thresholds*—On ports with WRED-drop thresholds, frames of a given CoS value are admitted to the queue based on a random probability designed to avoid buffer congestion. The probability of a frame with a given CoS being admitted to the queue or discarded depends on the weight and threshold assigned to that CoS value.

  For example, if CoS 2 is assigned to queue 1, threshold 2, and the threshold 2 watermarks are 40 percent (low) and 80 percent (high), frames with CoS 2 will not be dropped until queue 1 is at least 40 percent full. As the queue depth approaches 80 percent, frames with CoS 2 have an increasingly higher probability of being discarded rather than being admitted to the queue. When the queue is more than 80 percent full, all CoS 2 frames are dropped until the queue is less than 80 percent full. The frames that the switch discards when the queue level is between the low and high thresholds are picked at random, rather than on a per-flow or FIFO basis. This method works well with protocols such as TCP which are capable of adjusting to periodic packet drops by backing off and adjusting their transmission window size.

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 0661
Doc: 3701

When referring to the individual queues and thresholds on a port, a terse nomenclature is used. This terminology describes the number of strict priority queues (if present), the number of standard queues, and the number of tail-drop or WRED thresholds within each of the standard queues. The different queue and threshold types on the Catalyst 6500 Series Ethernet modules are shown in Table 1.

Table 1 Receive and Transmit Port Queue and Drop Threshold Types on Catalyst 6500 Series Ethernet Modules

Port Queue and Drop Threshold Structure with QoS	Description
Receive Queues	
1q4t	One standard queue with four tail-drop thresholds
1p1q4t	One strict-priority queue, one standard queue with four tail-drop thresholds
1p1q0t	One strict-priority queue, one standard queue with one nonconfigurable (100%) tail-drop threshold
1p1q8t	One strict-priority queue, one standard queue with eight configurable WRED-drop thresholds and one nonconfigurable (100%) tail-drop threshold
Transmit Queues	
2q2t	Two standard queues with two tail-drop thresholds per queue
1p2q2t	One strict-priority queue, two standard queues with two WRED-drop thresholds per queue
1p3q1t	One strict-priority queue, three standard queues with one WRED-drop threshold and one nonconfigurable tail-drop threshold per queue
1p2q1t	One strict-priority queue, two standard queues with one WRED-drop threshold and one nonconfigurable (100%) tail-drop threshold per queue

Buffer Sizes, Queues, and Thresholds by Ethernet Module

Table 2 provides the following information for each of the Catalyst 6500 Series Ethernet modules:

- Total buffer size per port (Total buffer size)
- Overall receive buffer size per port (Rx buffer size)
- Overall transmit buffer size per port (Tx buffer size)
- Port receive queue and drop threshold structure (Rx port type)
- Port transmit queue and drop threshold structure (Tx port type)
- Default size of receive buffers per queue with QoS enabled (Rx queue sizes)
- Default size of transmit buffers per queue with QoS enabled (Tx queue sizes)

Cisco Systems, Inc.
All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0662
Fls:
Doc: 3701

Table 2 Buffer Sizes, Queues, and Thresholds by Ethernet Module

Module Model Name	Module Description	Total Buffer Size	Rx Buffer Size	Tx Buffer Size	Rx Port Type	Tx Port Type	Rx Queue Sizes	Tx Queue Sizes
Supervisor Engine Modules (Gigabit Ethernet uplink ports)								
WS-X6K-S2U-MSFC2 WS-X6K-S2-MSFC2 WS-X6K-S2-PFC2	All Supervisor Engine 2 uplink ports	512 KB	73 KB	439 KB	1p1q4t	1p2q2t	SP—9 KB Q1—64 KB	SP—64 KB Q2—64 KB Q1—311 KB
WS-X6K-S1A-MSFC2 WS-X6K-SUP1A-MSFC WS-X6K-SUP1A-PFC WS-X6K-SUP1A-2GE	All Supervisor Engine 1A uplink ports	512 KB	73 KB	439 KB	1p1q4t	1p2q2t	SP—9 KB Q1—64 KB	SP—64 KB Q2—64 KB Q1—311 KB
WS-X6K-SUP1-2GE	Supervisor Engine 1 uplink ports	512 KB	80 KB	432 KB	1q4t	2q2t	Q1—80 KB	Q2—80 KB Q1—352 KB
Ethernet and Fast Ethernet Modules								
WS-X6524-100FX-MM	24-port 100BASE-FX fabric-enabled with MT-RJ connectors	1116 KB	28 KB	1088 KB	1p1q0t	1p3q1t	SP—6 KB Q1—22 KB	SP—272 KB Q3—272 KB Q2—272 KB Q1—272 KB
WS-X6548-RJ-21	48-port 10/100BASE-TX fabric-enabled with RJ-21 connectors	1116 KB	28 KB	1088 KB	1p1q0t	1p3q1t	SP—6 KB Q1—22 KB	SP—272 KB Q3—272 KB Q2—272 KB Q1—272 KB
WS-X6548-RJ-45	48-port 10/100BASE-TX fabric-enabled with RJ-45 connectors	1116 KB	28 KB	1088 KB	1p1q0t	1p3q1t	SP—6 KB Q1—22 KB	SP—272 KB Q3—272 KB Q2—272 KB Q1—272 KB
WS-X6324-100FX-MM	24-port 100BASE-FX with MT-RJ connectors	128 KB	16 KB	112 KB	1q4t	2q2t	Q1—16 KB	Q2—22 KB Q1—90 KB
WS-X6324-100FX-SM	24-port 100BASE-FX with MT-RJ connectors	128 KB	16 KB	112 KB	1q4t	2q2t	Q1—16 KB	Q2—22 KB Q1—90 KB
WS-X6348-RJ-45	48-port 10/100BASE-TX with RJ-45 connectors	128 KB	16 KB	112 KB	1q4t	2q2t	Q1—16 KB	Q2—22 KB Q1—90 KB
WS-X6348-RJ21V	48-port 10/100BASE-TX with RJ-21 connectors and inline power	128 KB	16 KB	112 KB	1q4t	2q2t	Q1—16 KB	Q2—22 KB Q1—90 KB
WS-X6348-RJ-45V	48-port 10/100BASE-TX with RJ-45 connectors and inline power	128 KB	16 KB	112 KB	1q4t	2q2t	Q1—16 KB	Q2—22 KB Q1—90 KB
WS-X6224-100FX-MT	24-port 100BASE-FX with MT-RJ connectors	64 KB	8 KB	56 KB	1q4t	2q2t	Q1—8 KB	Q2—16 KB Q1—40 KB

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

ROS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 0663
Doc: 3701

Table 2 Buffer Sizes, Queues, and Thresholds by Ethernet Module

Module Model Name	Module Description	Total Buffer Size	Rx Buffer Size	Tx Buffer Size	Rx Port Type	Tx Port Type	Rx Queue Sizes	Tx Queue Sizes
WS-X6248-RJ-45	48-port 10/100BASE-TX with RJ-45 connectors	64 KB	8 KB	56 KB	1q4t	2q2t	Q1—8 KB	Q2—16 KB Q1—40 KB
WS-X6248-TEL	48-port 10/100BASE-TX with RJ-21 connectors	64 KB	8 KB	56 KB	1q4t	2q2t	Q1—8 KB	Q2—16 KB Q1—40 KB
WS-X6248A-TEL	48-port 10/100BASE-TX with RJ-21 connectors	128 KB	16 KB	112 KB	1q4t	2q2t	Q1—16 KB	Q2—22 KB Q1—90 KB
WS-X6148-RJ-45V	48-port 10/100BASE-TX with RJ-45 connectors and inline power	128 KB	16 KB	112 KB	1q4t	2q2t	Q1—16 KB	Q2—22 KB Q1—90 KB
WS-X6148-RJ21V	48-port 10/100BASE-TX with RJ-21 connectors and inline power	128 KB	16 KB	112 KB	1q4t	2q2t	Q1—16 KB	Q2—22 KB Q1—90 KB
WS-X6024-10FL-MT	24-port 10BASE-FL with MT-RJ connectors	64 KB	8 KB	56 KB	1q4t	2q2t	Q1—8 KB	Q2—16 KB Q1—40 KB
Gigabit Ethernet Modules								
WS-X6816-GBIC	16-port 1000BASE-X dual-fabric with GBIC connectors and onboard DFC	512 KB	73 KB	439 KB	1p1q4t	1p2q2t	SP—9 KB Q1—64 KB	SP—64 KB Q2—64 KB Q1—311 KB
WS-X6516-GBIC	16-port 1000BASE-X with GBIC connectors	512 KB	73 KB	439 KB	1p1q4t	1p2q2t	SP—9 KB Q1—64 KB	SP—64 KB Q2—64 KB Q1—311 KB
WS-X6516-GE-TX	16-port 10/100/1000BASE-T with RJ-45 connectors	512 KB	73 KB	439 KB	1p1q4t	1p2q2t	SP—9 KB Q1—64 KB	SP—64 KB Q2—64 KB Q1—311 KB
WS-X6408-GBIC	8-port 1000BASE-X with GBIC connectors	512 KB	80 KB	432 KB	1q4t	2q2t	Q1—80 KB	Q2—80 KB Q1—352 KB
WS-X6408A-GBIC	8-port 1000BASE-X with GBIC connectors	512 KB	73 KB	439 KB	1p1q4t	1p2q2t	SP—9 KB Q1—64 KB	SP—64 KB Q2—64 KB Q1—311 KB
WS-X6416-GBIC	16-port 1000BASE-X with GBIC connectors	512 KB	73 KB	439 KB	1p1q4t	1p2q2t	SP—9 KB Q1—64 KB	SP—64 KB Q2—64 KB Q1—311 KB
WS-X6416-GE-MT	16-port 1000BASE-SX with MT-RJ connectors	512 KB	73 KB	439 KB	1p1q4t	1p2q2t	SP—9 KB Q1—64 KB	SP—64 KB Q2—64 KB Q1—311 KB
WS-X6316-GE-TX	16-port 1000BASE-T with RJ-45 connectors	512 KB	73 KB	439 KB	1p1q4t	1p2q2t	SP—9 KB Q1—64 KB	SP—64 KB Q2—64 KB Q1—311 KB

Cisco Systems, Inc.
All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS Nº 03/2005 - CN -
CPMI - CORREIOS
Fls: 0664
Doc: 3701

Table 2 Buffer Sizes, Queues, and Thresholds by Ethernet Module

Module Model Name	Module Description	Total Buffer Size	Rx Buffer Size	Tx Buffer Size	Rx Port Type	Tx Port Type	Rx Queue Sizes	Tx Queue Sizes
10-Gigabit Ethernet Modules								
WS-X6502-10GE	1-port 10 GbE with OIM connectors	64.2 MB	256 KB	64 MB	1p1q8t	1p2q1t	51 KB 205 KB	SP—15.3 MB Q2—17.9 MB Q1—30.7 MB
WS-X6501-10GEX4	1-port 10 GbE with SC connectors	64.2 MB	256 KB	64 MB	1p1q8t	1p2q1t	51 KB 205 KB	SP—15.3 MB Q2—17.9 MB Q1—30.7 MB
Optical Services Modules								
OSM-*	All optical services modules (Layer 2 GE ports only)	512 KB	73 KB	439 KB	1p1q4t	1p2q2t	SP—9 KB Q1—64 KB	SP—64 KB Q2—64 KB Q1—311 KB

[1] This document only discusses the four "standard" Gigabit Ethernet ports present on most of the OSMs. It does not discuss the 4-port GE-WAN OSM or any other OSM-related interfaces.

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

All contents are Copyright © 1992–2003, Cisco Systems, Inc. All rights reserved. Catalyst, Cisco, Cisco IOS, Cisco Systems, and the Cisco Systems logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0208R)

LW4072 01/03

RQS N° 03/2005 - CN - CPMI - CORREIOS
0665
Fls:
3701
Doc:

BL

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0666
Fls:
Doc: 3701

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:

- Understanding How EtherChannel Works, page 6-1
- Understanding EtherChannel Frame Distribution, page 6-2
- Port Aggregation Control Protocol and Link Aggregation Control Protocol, page 6-2
- EtherChannel Configuration Guidelines, page 6-3
- Understanding the Port Aggregation Protocol, page 6-5
- Configuring EtherChannel Using PAgP, page 6-7
- Understanding the Link Aggregation Control Protocol, page 6-12
- Configuring EtherChannel Using LACP, page 6-14

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.

RQS Nº 03/2005 - CN - CORREIOS
Fls: 0667
3701
Doc:

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.

RQS Nº 03/2005 - CN - CPMI - CORREIOS
Fls: 0668
Doc:
3791

- 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.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0669
Fls: 3701
Doc:

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)
```


RQS Nº 03/2005 - CN - CORREIOS
0670
Fls:
3701
Doc:

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."

RQS Nº 03/2005 - CN - CPMI - CORREIOS
0671
Fls:
3701
Doc:

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)
```


RCT 3470
ROS N8 03/2005 - CN
CPMI - 6-11 IOS
0672
FIs:
3701
Doc:

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 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 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

RQS Nº 03/2005 - CN
CPMI - 6-13 OS
0673
Fls:
Doc: 3701

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 Priority, 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.

pecifying 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*

ROS-Nº 03/2005 - CN
CPMI - 6.15 OS
0674
Fls:
3701
Doc:

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

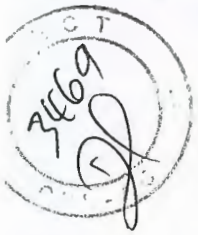
You can accomplish this task using a global command that configures both LACP and PAgP. For more information, see the "Setting the EtherChannel VLAN Cost" section on page 6-9.

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.

RQS Nº 03/2005 - CN - CPMI - CORREIOS
Fls: 0675
Doc: 3701

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)
```

ECT 3468 CPL AC

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>
```


ROS N° 03/2005 - CN
CPMI - CORREIOS 6.19
Fls: 0676
Doc: 3701

Ap BM

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0677
Fls:
Doc: 3701

Cisco Content Switching Module for the Cisco Catalyst 6500 and Cisco 7600 Internet Router

Product Overview

The Cisco Content Switching Module (CSM) is a Cisco Catalyst 6500 line card that balances client traffic to farms of servers, firewalls, SSL devices, caches, or 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 by 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:

- Market-leading performance

  Establishes up to 160,000 Layer 4 connections per second (performance may vary based upon software versions being run) and provides high-speed content switching, while maintaining 1 million concurrent connections.

- Outstanding price/performance value for enterprises and ISPs

  Features a low connection cost and occupies a small footprint. The Cisco CSM slides into a slot in a new or existing Cisco Catalyst 6500 and enables all ports in the Cisco Catalyst 6500 for layer 4 through layer 7 content switching. Multiple Cisco CSMs can be installed in the same Cisco Catalyst 6500.

- Ease of configuration

  Uses the same Cisco IOS Command Line Interface (CLI) that is used to configure the Cisco Catalyst 6500 Switch.

Key Features and Benefits

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. The Cisco CSM supports both stealth and regular firewalls.

URL and Cookie-based Load Balancing

The Cisco CSM allows full regular expression pattern matching for policies based on URLs, cookies, and 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 160,000 new Layer 4 TCP connection setups per second (performance may vary based upon software versions being run). These connections can be spread across 4096 virtual services (16,384 real servers) and all of 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 all of the ports to be used 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.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1
Fls: 0678
Doc: 3701

IP Protocol Support

The Cisco CSM accommodates a wide range of common IP protocols—including TCP, User Datagram Protocol (UDP). Additionally, the Cisco CSM supports higher-level protocols, including Hypertext Transfer Protocol (HTTP), File Transfer Protocol (FTP), Telnet, Dynamic Name Server (DNS), and Simple Mail Transfer Protocol (SMTP). The Cisco CSM also can handle UDP fragments and assemble them, regardless of the order in which they were received.

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. The Cisco CSM's User Session Stickiness provides the ability to consistently bring users back to the same server-based on Secure Socket Layer (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 leverages the robust 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 application availability using Health Monitoring probes, Inband health monitoring, return code checking, scriptable health checks and the Dynamic Feedback Protocol (DFP). SNMP server health traps can also be configured to monitor real server, virtual server, and fault tolerant state changes. 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. In the event the active Cisco CSM fails, open connections are handled by the standby Cisco CSM without interruption, and users will experience hitless failover—an important requirement for e-commerce sites and sites where encryption is used.

Global Server Load Balancing

Global Server load Balancing (GSLB) is used as a method to enhance the user experience by distributing content geographically for efficient delivery of content and additionally for disaster recovery. The Cisco CSM employs GSLB technology to communicate directly with Cisco Distributed Director in both global and geographical load balanced environments. The Cisco CSM GSLB functionality can be configured to act as an authoritative DNS, which lets it collect load information from other Cisco CSMs in the network. This information is then used to load balance incoming traffic across

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 0679
3701
Doc:

the geographically dispersed Cisco CSMs. The Cisco CSM can also interoperate with the Global Site Selector (GSS) by acting as the authoritative DNS and feeding it load information for its virtual IPs. An additional software feature license is required to enable GSLB support in the Cisco CSM.

Specifications

Hardware

Table 21-124: Specifications for the Cisco Content Switching Module

Description	Specification
Configuration limits	256 total VLANs (client and server) 4,000 virtual servers 4,000 server farms 16,000 real servers 4,000 probes 16,000 access control list (ACL)
Performance—connections	1,000,000 concurrent TCP connections 160,000 connection setups per second-Layer 4 [1] 80,000 connection setups per second-Layer 7 [1]
Performance—throughput	4 Gigabits-per-second total combined (client-to-server and server-to-client)
Platform requirements	Native Cisco IOS Software only Multilayer switch feature card—MSFC or MSFC2 Functions as a "classic" line card, not fabric enabled
Physical specifications	Occupies a 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) Storage temperature: –40 to 158°F (–40 to 70°C) Operating relative humidity: 10 to 90% (noncondensing) Storage relative humidity: 5 to 95% (noncondensing) Operating and storage altitude: Sea level to 10,000 ft. (3050 m)
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

1. Performance may vary based upon software versions being run.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
3
0680
Fls:
Doc: 3701

Software

Table 21-125: Software Release Requirements for Cisco Content Switching Module

Cisco CSM Software Release	Hardware Part Number	Software Part Number	Hardware Requirements	Native IOS Release	Added Features
1.2	WS-X6066-SLB-APC	sc6k-1.2-CSM=	Supervisor 1A with MSFC and PFC -Or- Supervisor 2 Module with MSFC 2	12.1(8a)e	• Supervisor 2 support • Route Health Injection
2.1(x)	WS-X6066-SLB-APC	sc6k-2.1-CSM=	Supervisor 1A with MSFC and PFC -Or- Supervisor 2 with MSFC 2	12.1(8a)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 CSM in a Chassis • VPN/IPsec Load Balancing
2.2(x)	WS-X6066-SLB-APC	Sc6k-2.2-CSM=	Supervisor 1A with MSFC and PFC -Or- Supervisor 2 with MSFC 2	12.1(11b)e	• Inband health monitoring • Return code checking • VLAN limit increased to 256 • RTSP support • Pending connection timeout value configuration
3.1(x)	WS-X6066-SLB-APC	Sc6k-3.1.1-CSM= Or Sc6k-3.1.1GSLB-CSM= [1]	Supervisor 1A with MSFC and PFC Or Supervisor 2 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 • Global Server Load Balancing [1] • Resource usage display • HTTP method parsing • Real Server Names • Non-TCP connection state redundancy • Reverse Sticky • SSL Services Module ID • Uni-directional Idle timeout

1. The Cisco CSM Global Server Load Balancing (GSLB) feature requires the purchase of an additional software feature license.

Ordering Information

Product Part Numbers

All part descriptions and part numbers for Cisco products can be accessed using the online Cisco Pricing Tool at

http://www.cisco.com/cgi-bin/front.x/pricing

The Cisco Pricing Tool requires a user name and password. If you are not already registered, go to

http://www.cisco.com/register and follow the instructions. After you have registered, you may access the Pricing Tool.

ECT 3463
DEC/MF Tool 09/2005 - CN
CPMI - CORREIOS
0681
Fls:
Doc: 3701

Ap BN

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0682
Fls:
3701
Doc:

CHAPTER 43

Configuring QoS

This chapter describes how to configure quality of service (QoS) on the Catalyst 6500 series switches and includes the configuration information that is required to support Common Open Policy Service (COPS) and Resource ReSerVation Protocol (RSVP).

Note

- For complete syntax and usage information for the commands used in this chapter, refer to the *Catalyst 6500 Series Switch Command Reference* publication.
- For information on using automatic QoS, see Chapter 44, "Using Automatic QoS."

You can configure QoS using one of the following:

- SNMP
- COPS protocol
- RSVP null service template and receiver proxy functionality
- Command-line interface (CLI)

This chapter consists of these sections:

- Understanding How QoS Works, page 43-1
- QoS Default Configuration, page 43-30
- Configuring QoS on the Switch, page 43-34

Understanding How QoS Works

Note

- Throughout this publication and all Catalyst 6500 series documents, the term "QoS" refers to the QoS feature as implemented on the Catalyst 6500 series.
- Supervisor Engine 1 and Supervisor Engine 2 provide policing only for ingress traffic.

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.

RQS Nº 03/2005 - CN - CPMI - CORREIOS

Fls: 0683

Doc: 3701

The QoS feature on the Catalyst 6500 series switches selects network traffic, prioritizes it according to its relative importance, and provides priority-indexed treatment through congestion avoidance techniques. Implementing QoS in your network makes network performance more predictable and bandwidth utilization more effective.

QoS sets Layer 2 and Layer 3 values in network traffic to a configured value or to a value based on received Layer 2 or Layer 3 values. IP traffic retains the Layer 3 value when it leaves the switch.

These sections describe QoS:

- QoS Terminology, page 43-2
- Flowcharts, page 43-4
- QoS Feature Set Summary, page 43-9
- Ethernet Ingress Port Marking, Scheduling, Congestion Avoidance, and Classification, page 43-10
- Classification, Marking, and Policing with a Layer 3 Switching Engine, page 43-16
- Classification and Marking with a Layer 2 Switching Engine, page 43-26
- Ethernet Egress Port Scheduling, Congestion Avoidance, and Marking, page 43-27
- QoS Statistics Data Export, page 43-30

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 that are carried in packets and frames:
  - Layer 2 class of service (CoS) values 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 CoS values.

    Note On ports that are configured as ISL trunks, all traffic is in ISL frames. On ports that are configured as 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 0 for low priority and 7 for high priority.

- Layer 3 differentiated services code point (DSCP) values—The Internet Engineering Task Force (IETF) defines the six most significant bits of the 1-byte ToS field as the DSCP. The priority represented by a particular DSCP value is configurable. DSCP values range between 0 and 63 (for more information, see the "Configuring DSCP Value Maps" section on page 43-61).

Note Layer 3 IP packets can carry either an IP precedence value or a DSCP value. QoS supports the use of either value, because DSCP values can be set equal to IP precedence values.

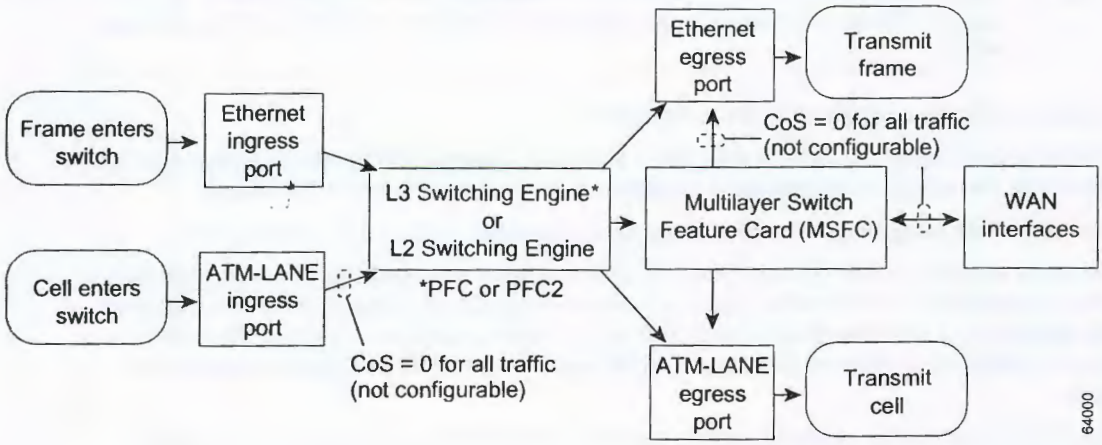
- *Classification* is the selection of traffic to be marked.
- *Marking*, according to RFC 2475, is the process of setting a Layer 3 DSCP value in a packet; in this publication, the definition of marking is extended to include setting Layer 2 CoS values.
- *Scheduling* is the assignment of traffic to a queue. QoS assigns traffic based on CoS values.
- *Congestion avoidance* is the process by which QoS reserves ingress and egress port capacity for traffic with high-priority CoS values. QoS implements congestion avoidance with CoS value-based drop thresholds. A drop threshold is the percentage of buffer utilization at which traffic with a specified CoS value is dropped, leaving the buffer available for traffic with higher-priority CoS values.
- *Policing* is the process by which the switch limits the bandwidth that is consumed by a flow of traffic. Policing can mark or drop traffic.
- Except where specifically differentiated, *Layer 3 switching engine* refers to either of the following:
  - Supervisor Engine 2 with Layer 3 Switching Engine II (Policy Feature Card 2 or PFC2)
  - Supervisor Engine 1 with Layer 3 Switching Engine WS-F6K-PFC (Policy Feature Card or PFC)
- Random early detection (RED) is a drop threshold algorithm.
- Weighted random early detection (WRED) is a drop threshold algorithm.
- Weighted round robin (WRR) is a dequeuing algorithm.
- Deficit weighted round robin (DWRR) is a dequeuing algorithm.

RQS Nº 03/2005 - CN
CORREIOS
Fls: 0684
Doc: 3701

Flowcharts

Figure 43-1 shows how traffic flows through the QoS features; Figure 43-2 through Figure 43-7 show more details of the traffic flow through QoS features.

Figure 43-1 Traffic Flow Through QoS Features



Note

- The PFC can provide Layer 3 switching for ingress WAN traffic. The PFC does not provide QoS for ingress WAN traffic. PFC QoS does not change the ToS byte in WAN traffic.
- Ingress LAN traffic that is Layer 3 switched does not go through the Multilayer Switch Feature Card (MSFC or MSFC2) and retains the CoS value that is assigned by the Layer 3 switching engine.
- Enter the **show port capabilities** command to see the queue structure of a port (for more information, see the "Receive Queues" section on page 43-12 and the "Transmit Queues" section on page 43-27).

Figure 43-2 Ethernet ingress Port Classification, Marking, Scheduling, and Congestion Avoidance

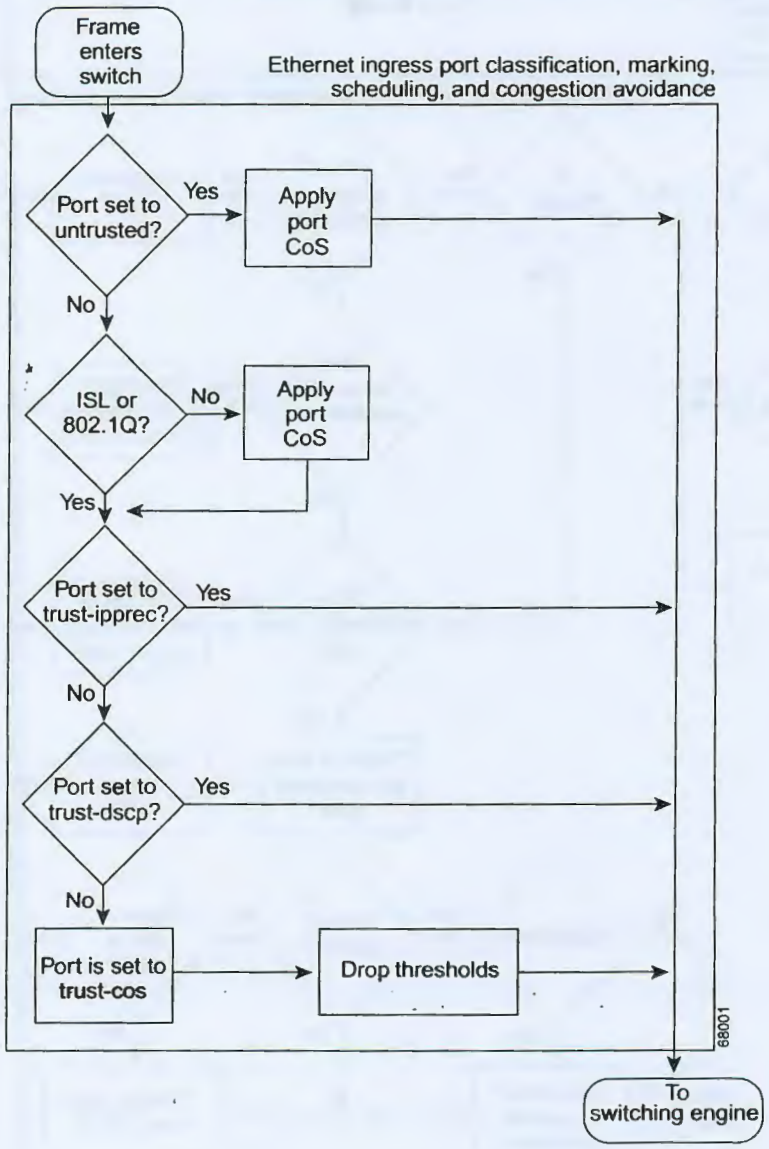
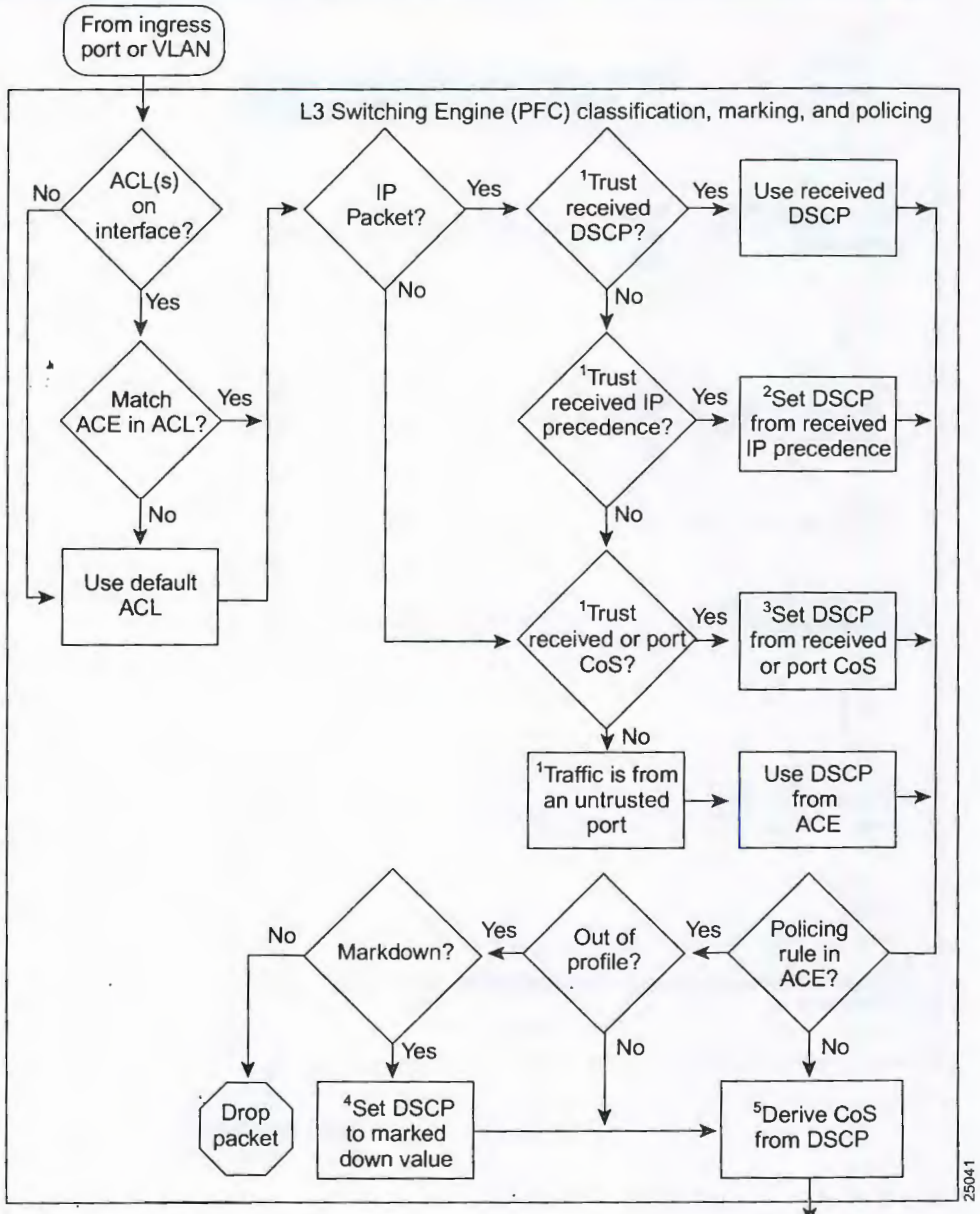


Figure 43-3 Layer 3 Switching Engine Classification, Marking, and Policing



[1] Specified by ACE keyword or by port keyword and **dscp** ACE keyword

[2] From IP precedence-to-DSCP map

[3] From CoS-to-DSCP map

[4] From DSCP markdown map

[5] From DSCP-to-CoS map

Figure 43-4 Layer 2 Switching Engine Classification and Marking

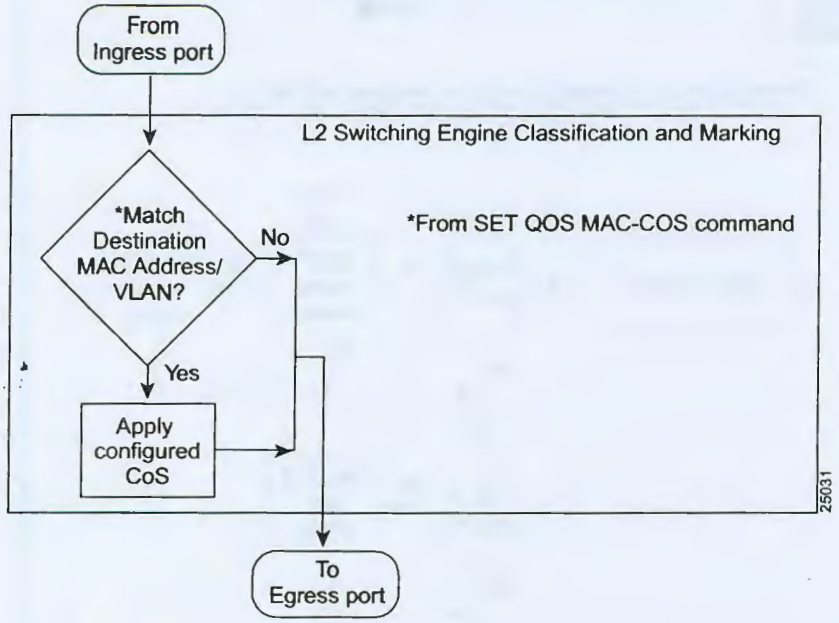
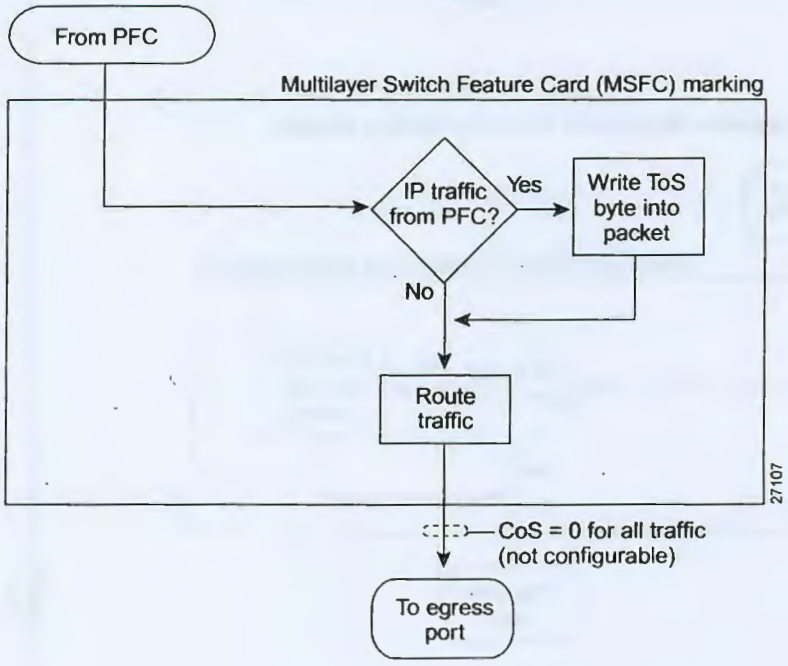


Figure 43-5 Multilayer Switch Feature Card Marking (MSFC and MSFC2)



RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 0686
Doc: 3701

Figure 43-6 Ethernet Egress Port Scheduling, Congestion Avoidance, and Marking

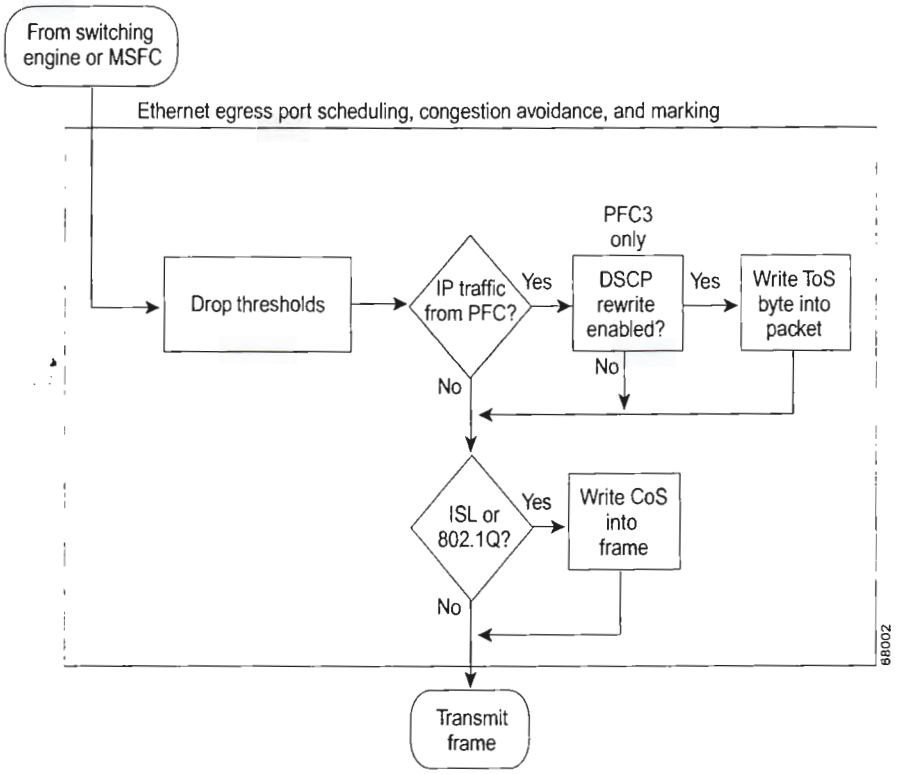
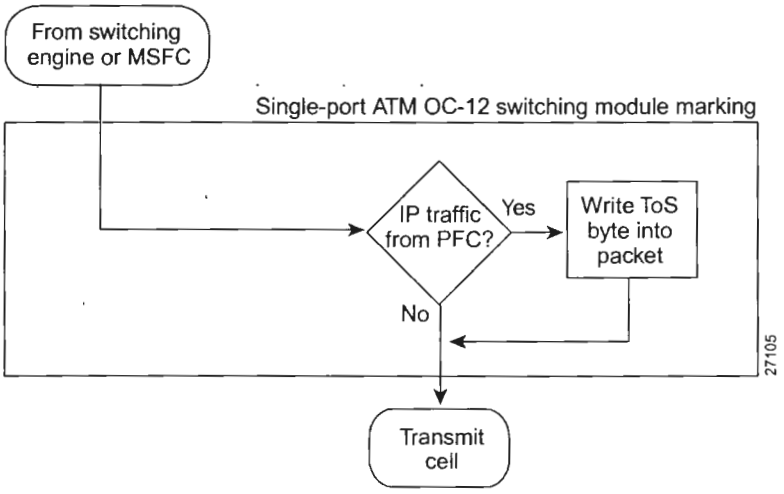


Figure 43-7 Single-Port ATM OC-12 Switching Module Marking



ECT 3454

QoS Feature Set Summary

The QoS feature set on your switch is determined by the switching engine on the supervisor engine. Enter the **show module** command for the supervisor engine to display your switching engine configuration. The display shows the "Sub-Type" to be one of the following:

- Supervisor Engine 2 (WS-X6K-SUP2-2GE) with Layer 3 Switching Engine II (WS-F6K-PFC2—Policy Feature Card 2 or PFC2)
- Supervisor Engine 1 (WS-X6K-SUP1A-2GE or WS-X6K-SUP1-2GE) with one of the following:
  - Layer 3 Switching Engine (WS-F6K-PFC—Policy Feature Card or PFC)
  - Layer 2 Switching Engine II (WS-F6020A)
  - Layer 2 Switching Engine I (WS-F6020)

The Layer 3 Switching Engine WS-F6K-PFC and Layer 3 Switching Engine II support similar feature sets. The two Layer 2 switching engines support the same QoS feature set.

These sections describe the QoS feature sets:

- Ethernet Ingress Port Features, page 43-9
- Layer 3 Switching Engine Features, page 43-9
- Layer 2 Switching Engine Features, page 43-10
- Ethernet Egress Port Features, page 43-10
- Single-Port ATM OC-12 Switching Module Features, page 43-10
- Multilayer Switch Feature Card (MSFC or MSFC2), page 43-10

Ethernet Ingress Port Features

With any switching engine, QoS supports classification, marking, scheduling, and congestion avoidance using Layer 2 CoS values at Ethernet ingress ports. Classification, marking, scheduling, and congestion avoidance at Ethernet ingress ports do not use or set Layer 3 IP precedence or DSCP values. With a Layer 3 switching engine, you can configure Ethernet ingress port trust states that can be used by the switching engine to set Layer 3 IP precedence or DSCP values and the Layer 2 CoS value. For more information, see the "Ethernet Ingress Port Marking, Scheduling, Congestion Avoidance, and Classification" section on page 43-10.

Layer 3 Switching Engine Features

With a Layer 3 switching engine, QoS supports classification, marking, and policing using IP, IPX, and Media Access Control (MAC) access control lists (ACLs). ACLs contain access control entries (ACEs) that specify Layer 2, 3, and 4 classification criteria, a marking rule, and policers. Marking sets the Layer 3 IP precedence or DSCP values and the Layer 2 CoS value to either received or configured Layer 2 or Layer 3 values. Policing uses bandwidth limits to either drop or mark nonconforming traffic. For more information, see the "Classification, Marking, and Policing with a Layer 3 Switching Engine" section on page 43-16.

During processing, a Layer 3 switching engine associates a DSCP value with all traffic, including non-IP traffic (for more information, see the "Internal DSCP Values" section on page 43-17).

RQS-Nº 03/2005 - CN
CPMI - CORREIOS
0687
Fls:
3701
Doc:

Layer 2 Switching Engine Features

With a Layer 2 Switching Engine, QoS can classify traffic using Layer 2 destination MAC addresses, VLANs, and marking using Layer 2 CoS values. Classification and marking with a Layer 2 Switching Engine do not use or set Layer 3 IP precedence or DSCP values. For more information, see the "Classification and Marking with a Layer 2 Switching Engine" section on page 43-26.

Ethernet Egress Port Features

With any switching engine, QoS supports Ethernet egress port scheduling and congestion avoidance using Layer 2 CoS values. Ethernet egress port marking sets Layer 2 CoS values and, with a Layer 3 switching engine, Layer 3 DSCP values. For more information, see the "Ethernet Egress Port Scheduling, Congestion Avoidance, and Marking" section on page 43-27.

Single-Port ATM OC-12 Switching Module Features

The ingress interface from a single-port ATM OC-12 switching module is untrusted, and QoS sets CoS to zero in all traffic received from it. With a Layer 3 switching engine, QoS can mark IP traffic that is transmitted to a single-port ATM OC-12 switching module with Layer 3 DSCP values.

Multilayer Switch Feature Card (MSFC or MSFC2)

QoS marks IP traffic that is transmitted to an MSFC with Layer 3 DSCP values. CoS is zero in all traffic that is sent from an MSFC to egress ports.

Note Traffic that is Layer 3 switched does not go through the MFSC and retains the CoS value that is assigned by the Layer 3 switching engine.

Ethernet Ingress Port Marking, Scheduling, Congestion Avoidance, and Classification

These sections describe Ethernet ingress port marking, scheduling, congestion avoidance, and classification:

- Overview, page 43-11
- Marking at Untrusted Ports, page 43-11
- Marking at Trusted Ports, page 43-11
- Ethernet Ingress Port Scheduling and Congestion Avoidance, page 43-12
- Receive Queues, page 43-12
- Ingress Scheduling, page 43-12
- Ingress Congestion Avoidance, page 43-12
- Ethernet Ingress Port Classification Features with a Layer 3 Switching Engine, page 43-15

Overview

The trust state of an Ethernet port determines how it marks, schedules, and classifies received traffic, and whether or not congestion avoidance is implemented. You can configure the trust state of each port with one of these keywords:

- **untrusted** (default)
- **trust-ipprec** (Layer 3 switching engine only—not supported on **1q4t** ports except Gigabit Ethernet)
- **trust-dscp** (Layer 3 switching engine only—not supported on **1q4t** ports except Gigabit Ethernet)
- **trust-cos**

Note

- **1q4t** ports (except Gigabit Ethernet) do not support the **trust-ipprec** and **trust-dscp** port keywords. You must configure a **trust-ipprec** or **trust-dscp** ACL that matches the ingress traffic to apply the **trust-ipprec** or **trust-dscp** trust state.
- On **1q4t** ports (except Gigabit Ethernet), the **trust-cos** port keyword displays an error message, activates receive queue drop thresholds, and—as indicated by the error message—does not apply the **trust-cos** trust state to traffic. You must configure a **trust-cos** ACL that matches the ingress traffic to apply the **trust-cos** trust state.

For more information, see the "Configuring the Trust State of a Port" section on page 43-36.

In addition to the port configuration keywords listed above, with a Layer 3 switching engine, QoS uses **trust-ipprec**, **trust-dscp**, and **trust-cos** ACE keywords. Do not confuse the ACE keywords with the port keywords.

Ports that are configured with the **untrusted** keyword are called untrusted ports. Ports that are configured with the **trust-ipprec**, **trust-dscp**, or **trust-cos** keywords are called trusted ports. QoS implements ingress port congestion avoidance only on ports that are configured with the **trust-cos** keyword.

Ingress port marking, scheduling, and congestion avoidance use Layer 2 CoS values. Ingress port marking, scheduling, and congestion avoidance do not use or set Layer 3 IP precedence or DSCP values.

Marking at Untrusted Ports

QoS marks all frames that are received through untrusted ports with the port CoS value (the default is zero). QoS does not implement ingress port congestion avoidance on untrusted ports: the traffic goes directly to the switching engine.

Marking at Trusted Ports

When an ISL frame enters the switch through a trusted port, 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 port, QoS accepts the User Priority bits as a CoS value. QoS marks all traffic that is received in other frame types with the port CoS value.

The port CoS value is configurable for each Ethernet port (for more information, see the "Configuring the CoS Value for a Port" section on page 43-37).

RQS Nº 03/2005 - CN
SPMI - CORREIOS
0688
Fls:
Doc: 3701

Ethernet Ingress Port Scheduling and Congestion Avoidance

QoS does not implement ingress port congestion avoidance on ports that are configured with the **untrusted**, **trust-ipprec**, or **trust-dscp** keywords: the traffic goes directly to the switching engine.

QoS uses CoS-value-based receive-queue drop thresholds to avoid congestion in traffic entering the switch through a port that is configured with the **trust-cos** keyword (for more information, see the "Configuring the Trust State of a Port" section on page 43-36).

Receive Queues

Enter the **show port capabilities** command to see the queue structure of a port. The command displays one of the following:

- **rx-(1q2t)** indicates one standard queue with one configurable tail-drop threshold and one nonconfigurable tail-drop threshold.
- **rx-(1q4t)** indicates one standard queue with four configurable tail-drop thresholds.
- **rx-(1p1q4t)** indicates one strict-priority queue and one standard queue with four configurable tail-drop thresholds.
- **rx-(1p1q0t)** indicates one strict-priority queue and one standard queue with a nonconfigurable threshold.
- **rx-(1p1q8t)** indicates one strict-priority queue and one standard queue with eight configurable WRED-drop thresholds (on **1p1q8t** ports, the standard queue also has one nonconfigurable tail-drop threshold).

Strict-priority queues are serviced in preference to other queues. QoS services traffic in a strict-priority queue before servicing the standard queue. When QoS services the standard queue, after receiving a packet, it checks for traffic in the strict-priority queue. If 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.

Ingress Scheduling

QoS schedules traffic through the receive queues based on CoS values. In the **1p1q4t**, **1p1q0t**, and **1p1q8t** default configurations, QoS assigns all traffic with CoS 5 to the strict-priority queue; QoS assigns all other traffic to the standard queue. In the **1q4t** default configuration, QoS assigns all traffic to the standard queue.

Ingress Congestion Avoidance

Note The explanations in this section use default values. You can configure many of the parameters (for more information, see the "Configuring QoS on the Switch" section on page 43-34). All ports of the same type use the same drop-threshold configuration.

If a port is configured with the **trust-cos** keyword, QoS implements CoS-value-based receive-queue drop thresholds to avoid congestion in received traffic.

1q2t 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 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 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 as follows:
  - 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 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 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 a nonconfigurable tail-drop threshold that drops incoming frames when the standard 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 as follows:
  - Using standard receive-queue 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 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.

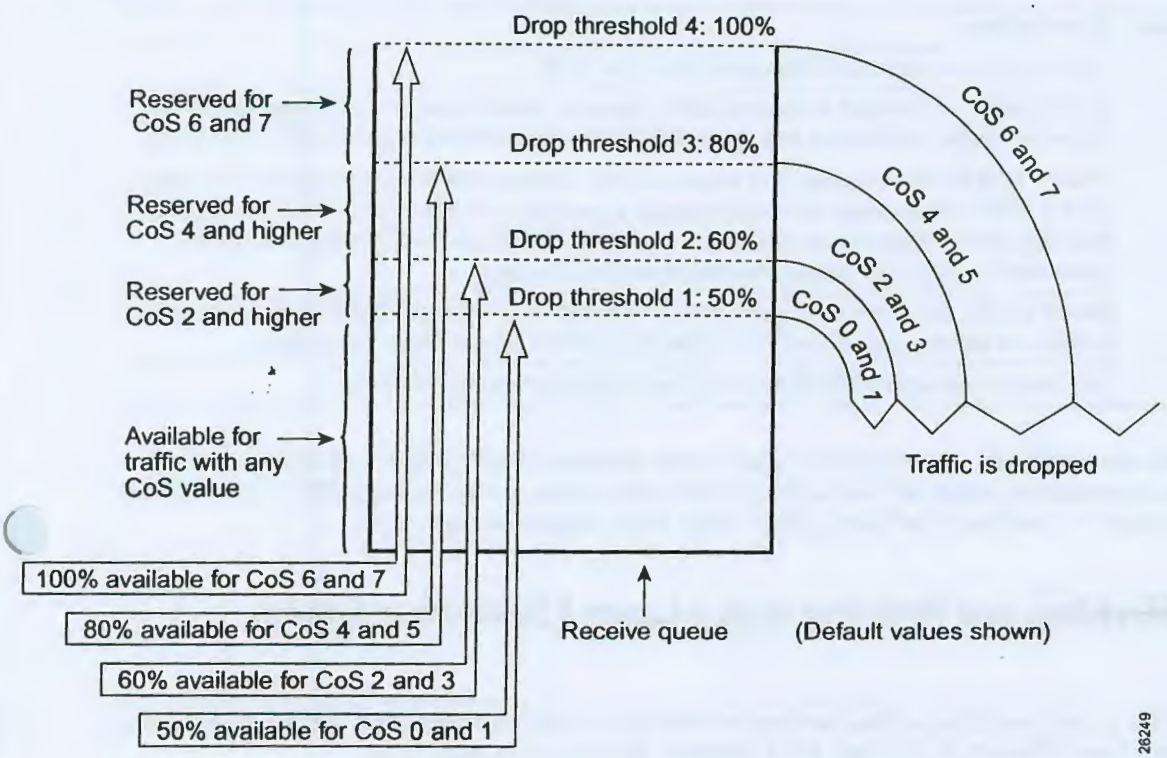
RQS Nº 03/2005 - CN
CPMI - CORREIOS
43-13
0689
Fls:
Doc: 3701

- Using standard receive-queue 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 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 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 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 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 the CoS values that are mapped only to the queue. The switch uses WRED-drop thresholds for traffic carrying the CoS values that are mapped to the queue and a threshold. See the "1p1q8t Receive Queues" section on page 43-60.

Figure 43-8 shows the drop thresholds for a **1q4t** port. Drop thresholds in other configurations function similarly.

Figure 43-8 Receive-Queue Drop Thresholds



Ethernet Ingress Port Classification Features with a Layer 3 Switching Engine

You can use the **untrusted**, **trust-ipprec**, **trust-dscp**, and **trust-cos** port keywords to classify traffic on a per-port basis for a Layer 3 switching engine to mark.

The **trust-ipprec** and **trust-dscp** keywords are supported only with a Layer 3 switching engine and are not supported on **1q4t** ports except Gigabit Ethernet. On **1q4t** ports (except Gigabit Ethernet), the **trust-cos** port keyword displays an error message, activates receive-queue drop thresholds, and—as indicated by the error message—does not apply the **trust-cos** trust state to traffic. You must configure the **trust-cos** ACL that matches the ingress traffic to apply the **trust-cos** trust state.

In addition to per-port classification, you can create ACEs that classify traffic on a per-packet basis (for IP and IPX traffic, see the "Named IP ACLs" section on page 43-42 and the "Creating or Modifying Named IPX ACLs" section on page 43-46) or on a per-frame basis (for other traffic, see the "Creating or Modifying Named MAC ACLs" section on page 43-47), regardless of the port configuration (see the "Marking Rules" section on page 43-23).

To mark traffic in response to per-port classification, the traffic must match an ACE that contains the **dscp** ACE keyword (see the "Marking Rules" section on page 43-23). In their default configuration, the ACEs in the default ACLs contain the **dscp** ACE keyword. Table 43-1 lists the per-port classifications and the marking rules that they invoke.

Table 43-1 Marking Based on Per-Port Classification

Port Keyword	ACE Keyword	Marking Rule
untrusted	**dscp**	Set internal and egress DSCP as specified in the ACE.
trust-ipprec	**dscp**	For IP traffic, set internal and egress DSCP from the received Layer 3 IP precedence value. For other traffic, set internal and egress DSCP from the received or port Layer 2 CoS value. **Note**—With the **trust-ipprec** port keyword, QoS uses only the IP precedence bits. If traffic with a DSCP value enters the switch through a port that is configured with the **trust-ipprec** port keyword, the three most significant bits of the DSCP value are interpreted as an IP precedence value; QoS ignores the rest of the DSCP value.
trust-dscp	**dscp**	For IP traffic, set internal and egress DSCP from the received Layer 3 DSCP value. For other traffic, set internal and egress DSCP from the received or port Layer 2 CoS value.
trust-cos	**dscp**	Set internal and egress DSCP from the received or port Layer 2 CoS value.

QoS uses configurable mapping tables to set internal and egress DSCP, which is a 6-bit value, from CoS and IP precedence, which are 3-bit values (for more information, see the "Internal DSCP Values" section on page 43-17 and the "Configuring DSCP Value Maps" section on page 43-61).

Classification, Marking, and Policing with a Layer 3 Switching Engine

Note With a Layer 3 switching engine, the Catalyst 6500 series switches provide QoS only for the following frame types: Ethernet_II, Ethernet_802.3, Ethernet_802.2, and Ethernet_SNAP.

These sections describe classification, marking, and policing with a Layer 3 switching engine:

- Internal DSCP Values, page 43-17
- ACLs, page 43-17
- Named ACLs, page 43-18
- Default ACLs, page 43-22
- Marking Rules, page 43-23
- Policers, page 43-24
- PFC2 Policing Decisions, page 43-25
- Attaching ACLs, page 43-26
- Final Layer 3 Switching Engine CoS and ToS Values, page 43-26

Note Classification with a Layer 3 switching engine uses Layer 2, 3, and 4 values. Marking with a Layer 3 switching engine uses Layer 2 CoS values and Layer 3 IP precedence or DSCP values.

ECT 3446 CPI-AT

Internal DSCP Values

These sections describe the internal DSCP values:

- Internal DSCP Sources, page 43-17
- Egress DSCP and CoS Sources, page 43-17

Internal DSCP Sources

During processing, the priority of all traffic (including non-IP traffic) is represented with an internal DSCP value. QoS derives the internal DSCP value from the following:

- For **trust-cos** traffic, from received or port Layer 2 CoS values (traffic from an untrusted port has the port CoS value and if traffic from an untrusted port matches a **trust-cos** ACL, QoS derives the internal DSCP value from the port CoS value)
- For **trust-ipprec** traffic, from received IP precedence values
- For **trust-dscp** traffic, from received DSCP values
- For **untrusted** traffic, from port CoS or configured DSCP values

The trust state of traffic is the trust state of the ingress port unless set otherwise by the matching ACE.

Note A **trust-cos** ACL cannot restore received CoS in traffic from untrusted ports. Traffic from untrusted ports always has the port CoS value.

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 43-61 or the "Mapping Received IP Precedence Values to Internal DSCP Values" section on page 43-62).

Egress DSCP and CoS Sources

For egress IP traffic, QoS creates a ToS byte from the internal DSCP value (which you can set equal to an IP precedence 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.

For all egress traffic, QoS uses a configurable mapping table to derive a CoS value from the internal DSCP value that is associated with traffic (see the "Mapping Internal DSCP Values to Egress CoS Values" section on page 43-62). QoS sends the CoS value to Ethernet egress ports for use in scheduling and to be written into ISL and 802.1Q frames.

ACLs

QoS uses ACLs that contain ACEs. The ACEs specify classification criteria, a marking rule, and policers. QoS compares received traffic to the ACEs in ACLs until a match occurs. When the traffic matches the classification criteria in an ACE, QoS marks and polices the packet as specified in the ACE and makes no further comparisons.

There are three ACL types: IP, and with a Layer 3 switching engine, IPX and MAC. QoS compares traffic of each type (IP, IPX, and MAC) only to the corresponding ACL type (see Table 43-2).

ROS Nº 03/2005 - CN
CPMI - CO
0691
Fls:
370
Doc:

Table 43-2 Supported Ethertype Field Values

ACL Type	Ethertype Field Value	Protocol
IP	0x0800	IP
IPX	0x8137 and 0x8138	IPX
MAC[1]	0x0600 and 0x0601	XNS
	0x0BAD and 0x0BAF	Banyan VINES
	0x6000-0x6009 and 0x8038-0x8042	DECnet
	0x809b and 0x80f3	AppleTalk

1. QoS MAC ACLs that do not include an ethertype parameter match traffic with any value in the ethertype field, which allows MAC-level QoS to be applied to any traffic except IP and IPX.

QoS supports user-created *named* ACLs, each containing an ordered list of ACEs, and user-configurable *default* ACLs, each containing a single ACE.

Named ACLs

You create a named ACL when you enter an ACE with a new ACL name. You add an ACE to an existing ACL when you enter an ACE with the name of the existing ACL.

You can specify the classification criteria for each ACE in a named ACL. The classification criteria can be specific values or wildcards (for more information, see the "Creating or Modifying ACLs" section on page 43-41).

These sections describe the classification criteria that can be specified in a named ACL:

- IP ACE Layer 3 Classification Criteria, page 43-18
- IP ACE Layer 4 Protocol Classification Criteria, page 43-19
- IP ACE Layer 4 TCP Classification Criteria, page 43-19
- IP ACE Layer 4 UDP Classification Criteria, page 43-20
- IP ACE Layer 4 ICMP Classification Criteria, page 43-20
- IP ACE Layer 4 IGMP Classification Criteria, page 43-21
- IPX ACE Classification Criteria, page 43-21
- MAC ACE Layer 2 Classification Criteria, page 43-22

IP ACE Layer 3 Classification Criteria

You can create IP ACEs that match traffic with specific Layer 3 values by including these Layer 3 parameters (see the "Named IP ACLs" section on page 43-42):

- IP source address and mask, entered as specific values or with the **any** keyword or with the **host** keyword and a host address.
- IP destination address and mask, entered as specific values or with the **any** keyword or with the **host** keyword and a host address.
- DSCP value (0–63) or IP precedence that is specified with a numeric value (0–7) or these keywords:
  - **Network** (IP precedence 7)
  - **Internet** (IP precedence 6)

- **Critical** (IP precedence 5)
- **Flash-override** (IP precedence 4)
- **Flash** (IP precedence 3)
- **Immediate** (IP precedence 2)
- **Priority** (IP precedence 1)
- **Routine** (IP precedence 0)

Note IP ACEs that do not include a DSCP or IP precedence value parameter match all DSCP or IP precedence values.

IP ACE Layer 4 Protocol Classification Criteria

You can create IP ACEs that match specific Layer 4 protocol traffic by including a Layer 4 protocol parameter (see the "IP ACLs for Other Layer 4 Protocols" section on page 43-45). You can specify the protocol numerically (0–255) or with these keywords: **ahp** (51), **eigrp** (88), **esp** (50), **gre** (47), **igrp** (9), **icmp** (1), **igmp** (2), **igrp** (9), **ip** (0), **ipinip** (4), **nos** (94), **ospf** (89), **pcp** (108), **pim** (103), **tcp** (6), or **udp** (17).

Note IP ACEs that do not include a Layer 4 protocol parameter or that include the **ip** keyword match all IP traffic.

IP ACE Layer 4 TCP Classification Criteria

You can create Transmission Control Protocol (TCP) ACEs that match traffic for specific TCP ports by including TCP source and/or destination port parameters (for more information, see the "IP ACEs for TCP Traffic" section on page 43-43). You can specify TCP port parameters numerically (0–65535) or with these keywords:

Keyword	Port		Keyword	Port		Keyword	Port		Keyword	Port
bgp	179		**ftp**	21		**lpd**	515		**telnet**	23
chargen	19		**ftp-data**	20		**nntp**	119		**time**	37
daytime	13		**gopher**	70		**pop2**	109		**uucp**	540
discard	9		**hostname**	101		**pop3**	110		**whois**	43
domain	53		**irc**	194		**smtp**	25		**www**	80
echo	7		**klogin**	543		**sunrpc**	111			
finger	79		**kshell**	544		**tacacs**	49			

Note TCP ACEs that do not include a Layer 4 TCP port parameter match all TCP traffic.

ROS Nº 03/2005 - CN
CPMI - 43-19 OS
0692
Fls:
Doc:

IP ACE Layer 4 UDP Classification Criteria

You can create User Datagram Protocol (UDP) ACEs that match traffic for specific UDP source and/or destination ports by including UDP port parameters (for more information, see the "IP ACEs for UDP Traffic" section on page 43-43). You can specify UDP port parameters numerically (0–65535) or with these keywords:

Keyword	Port		Keyword	Port		Keyword	Port		Keyword	Port
biff	512		echo	7		rip	520		talk	517
bootpc	68		mobile-ip	434		snmp	161		tftp	69
bootps	67		nameserver	42		snmptrap	162		time	37
discard	9		netbios-dgm	138		sunrpc	111		who	513
dns	53		netbios-ns	137		syslog	514		xdmcp	177
dnsix	195		ntp	123		tacacs	49			

Note UDP ACEs that do not include a Layer 4 UDP port parameter match all UDP traffic.

IP ACE Layer 4 ICMP Classification Criteria

You can create Internet Control Management Protocol (ICMP) ACEs that match traffic containing specific ICMP messages by including ICMP types and optionally, ICMP codes (for more information, see the "IP ACEs for ICMP Traffic" section on page 43-44). You can specify ICMP types and codes numerically (0–255) or with these keywords:

Keyword	Type	Code	Keyword	Type	Code
administratively-prohibited	3	13	net-tos-unreachable	3	11
alternate-address[1]	6	—	net-unreachable	3	0
conversion-error	31	0	network-unknown	3	6
dod-host-prohibited	3	10	no-room-for-option	12	2
dod-net-prohibited	3	9	option-missing	12	1
echo	8	0	packet-too-big	3	4
echo-reply	0	0	parameter-problem	12	0
general-parameter-problem[1]	12	—	port-unreachable	3	3
host-isolated	3	8	precedence-unreachable	3	15
host-precedence-unreachable	3	14	protocol-unreachable	3	2
host-redirect	5	1	reassembly-timeout	11	1
host-tos-redirect	5	3	redirect[1]	5	—
host-tos-unreachable	3	12	router-advertisement	9	0
host-unknown	3	7	router-solicitation	10	0
host-unreachable	3	1	source-quench	4	0
information-reply	16	0	source-route-failed	3	5

E C T
2462
CPL - AC

Keyword	Type	Code	Keyword	Type	Code
information-request	15	0	**time-exceeded**[1]	11	—
mask-reply	18	0	**timestamp-reply**	14	0
mask-request	17	0	**timestamp-request**	13	0
mobile-redirect	32	0	**traceroute**	30	0
net-redirect	5	0	**ttl-exceeded**	11	0
net-tos-redirect	5	2	**unreachable**[1]	3	—

1. Matches all code values

Note ICMP ACEs with only a Layer 4 ICMP *type* parameter match all *code* values for that *type* value. ICMP ACEs that do not include any Layer 4 ICMP type and code parameters match all ICMP traffic.

IP ACE Layer 4 IGMP Classification Criteria

You can create IGMP ACEs that match traffic containing specific IGMP messages by including an IGMP type parameter (for more information, see the "IP ACEs for IGMP Traffic" section on page 43-44). You can specify the IGMP type numerically (0–255) or with these keywords: **host-query** (1), **host-report** (2), **dvmrp** (3), **pim** (4), or **trace** (5).

Note QoS does not support IGMP traffic when IGMP snooping is enabled. QoS supports IGMP classification using version 1 four-bit Type fields.

Note IGMP ACEs that do not include a Layer 4 IGMP type parameter match all IGMP traffic.

IPX ACE Classification Criteria

You can create IPX ACEs that match specific IPX traffic by including these parameters (for more information, see the "Creating or Modifying Named IPX ACLs" section on page 43-46):

- IPX source network (-1 matches any network number)
- Protocol, which can be specified numerically (0–255) or with these keywords: **any**, **ncp** (17), **netbios** (20), **rip** (1), **sap** (4), **spx** (5)
- IPX ACEs support the following optional parameters:
  - IPX destination network (-1 matches any network number)
  - If you specify an IPX destination network, IPX ACEs support the following optional parameters: an IPX destination network mask (-1 matches any network number), an IPX destination node, and an IPX destination node mask

ROS Nº 03/2005 - CN
CPMI - 43-21 IOS
Fls: 0693
Doc: 3701

MAC ACE Layer 2 Classification Criteria

You can create MAC ACEs that match specific Ethernet traffic by including these Layer 2 parameters (for more information, see the "Creating or Modifying Named MAC ACLs" section on page 43-47):

- Ethernet source and destination addresses and masks, entered as specific values or with the **any** keyword or with the **host** keyword and a host Ethernet address
- Optionally, an ethertype parameter from this list:
  - 0x809B (or **ethertalk**)
  - 0x80F3 (or **aarp**)
  - 0x6001 (or **dec-mop-dump**)
  - 0x6002 (or **dec-mop-remote-console**)
  - 0x6003 (or **dec-phase-iv**)
  - 0x6004 (or **dec-lat**)
  - 0x6005 (or **dec-diagnostic-protocol**)
  - 0x6007 (or **dec-lavc-sca**)
  - 0x6008 (or **dec-amber**)
  - 0x6009 (or **dec-mumps**)
  - 0x8038 (or **dec-lanbridge**)
  - 0x8039 (or **dec-dsm**)
  - 0x8040 (or **dec-netbios**)
  - 0x8041 (or **dec-msdos**)
  - 0x8042 (no keyword)
  - 0x0BAD (no keyword)
  - 0x0baf (or **banyan-vines-echo**)
  - 0x0600 (or **xerox-ns-idp**)

QoS MAC ACLs that do not include an ethertype parameter match traffic with any value in the ethertype field, which allows MAC-level QoS to be applied to any traffic except IP and IPX.

Default ACLs

There are three default ACLs, one each for IP, and with a Layer 3 switching engine, IPX and MAC traffic. Each ACL has a single ACE that has a configurable marking rule and configurable policers. The default ACLs have nonconfigurable classification criteria that matches all traffic. QoS compares any traffic with a supported ethertype field value that does not match a named ACL to the default ACLs. Unmatched IP traffic matches the default IP ACL. Unmatched IPX traffic matches the default IPX ACL. Unmatched Ethernet traffic matches the default MAC ACL.

Note All traffic matches an ACE in an ACL (either an ACE in a named ACL or one of the default ACLs) because the default ACLs match all traffic.

ECT 3440 CPI/AC

Marking Rules

Note Marking is not supported for IPX or MAC traffic with a PFC2.

Marking rules specify how QoS marks traffic when the traffic matches the filtering parameters in an ACE (see the "ACE Name, Marking Rule, Policing, and Filtering Syntax" section on page 43-41). QoS supports four marking rules, that are specified with the following four ACE keywords: **trust-dscp**, **trust-ipprec**, **trust-cos**, and **dscp**. Each ACE contains one of the keywords. The marking rules are as follows:

- **trust-dscp** (IP ACLs only)—Instructs QoS to set internal and egress DSCP from received DSCP values (see the "Internal DSCP Values" section on page 43-17).
- **trust-ipprec** (IP ACLs only)—Instructs QoS to set internal and egress DSCP from received IP precedence values.

  Note With the **trust-ipprec** port keyword, QoS uses only the IP precedence bits. If traffic with a DSCP value enters the switch through a port that is configured with the **trust-ipprec** port keyword, the three most significant bits of the DSCP value are interpreted as an IP precedence value; QoS ignores the rest of the DSCP value.

- **trust-cos** (all ACLs except IPX and MAC with a PFC2)—Instructs QoS to set internal and egress DSCP from received or port CoS values. In traffic from ports that are configured with the **trust-cos** keyword, the CoS value is received in ISL and 802.1Q frames; in all other cases, the CoS value is configured on the port (the default is zero).
- **dscp** (all ACLs except IPX and MAC with a PFC2)—Instructs QoS to mark traffic as indicated by the port trust keywords:
  - In IP traffic from ingress ports that are configured with the **trust-dscp** port keyword, the **dscp** ACE keyword instructs QoS to set the internal and egress DSCP values from the received DSCP values. In non-IP traffic, QoS sets the DSCP from the received or port CoS value.
  - In IP traffic from ingress ports that are configured with the **trust-ipprec** port keyword, the **dscp** ACE keyword instructs QoS to set the internal and egress DSCP values from the received IP precedence values. In non-IP traffic, QoS sets the DSCP value from the received or port CoS value.
  - In traffic from ingress ports that are configured with the **trust-cos** port keyword, the **dscp** ACE keyword instructs QoS to set the internal and egress DSCP values from the received or port CoS values.
  - In traffic from ingress ports that are configured with the **untrusted** port keyword, the **dscp** ACE keyword instructs QoS to set the internal and egress DSCP values from the DSCP value in the ACE.

    Note The default configuration of the ACEs in the default ACLs contains the **dscp** ACE keyword, which supports per-port classification of traffic. With the default values, the ACEs in the default ACLs apply DSCP zero to traffic from ingress ports that are configured with the **untrusted** port keyword.

ROSN° 08/2005 - CN
CPMI - C 43-23
0694
Fls: 3701
Doc:

QoS uses configurable mapping tables to set the DSCP value, which is 6 bits, from CoS and IP precedence, which are 3-bit values (for more information, see the "Mapping Received CoS Values to Internal DSCP Values" section on page 43-61 and the "Mapping Received IP Precedence Values to Internal DSCP Values" section on page 43-62).

Policers

You can create named policers that specify bandwidth utilization limits, which you can apply to traffic by including the policer name in an ACE (for more information, see the "Creating Policers" section on page 43-38).

Policing uses a token bucket scheme. As packets arrive, the packet size in bytes is added to the bucket level. Every 0.25 ms, a value equal to the token rate is subtracted from the bucket level.

You specify the bandwidth utilization limits as an average rate and a maximum burst size. Packets that exceed these limits are "out of profile." Traffic is in profile as long as it flows in at an average rate and never bursts beyond the burst size.

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"). Since out-of-profile packets do not retain their original priority, they are not counted as part of the bandwidth that is consumed by in-profile packets.

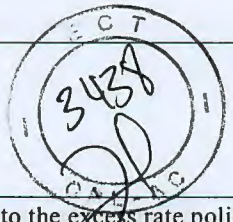
For all policers, QoS uses a configurable table that maps received DSCP values to marked-down DSCP values (for more information, see the "Mapping DSCP Markdown Values" section on page 43-63). When markdown occurs, QoS gets the marked-down DSCP value from the table. You cannot specify a marked-down DSCP value 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 received DSCP values. To enable markdown, configure the table appropriately for your network.

You give each policer a unique name when you create it and then use the name to include the policer in an ACE. The same policer can be used in multiple ACEs.

You can create these policers:

- Microflow—QoS applies the bandwidth limit that is specified in a microflow policer separately to each flow that matches any ACEs that use that particular microflow policer. You can create up to 63 microflow policers.
- Aggregate—QoS applies the bandwidth limits that are specified in an aggregate policer cumulatively to all flows that match any ACEs that use that particular aggregate policer. You can create up to 1023 aggregate policers.
- With a PFC2, you can specify a dual rate aggregate policer with a normal rate and an excess rate:
  - Normal rate—Packets exceeding this rate are marked down.
  - Excess rate—Packets exceeding this rate are either marked down or dropped as specified by the drop indication flag.



Note The drop indication flag applies to the excess rate policer and cannot be set for the normal rate policer. To achieve the effect of a drop indication flag for the normal rate aggregate policer, set the excess rate equal to the normal rate and set the drop indication flag. Alternatively, you can set the normal rate without specifying an excess rate, which automatically sets the excess rate to the normal rate when the drop indicator flag is on.

You can include both a microflow policer and an aggregate policer in each ACE to police a flow based on both its own bandwidth utilization and on its bandwidth utilization combined with that of other flows.

For example, you could create a microflow policer named "group_individual" with bandwidth limits that are suitable for individuals in a group and you could create an aggregate policer named "group_all" with bandwidth limits that are suitable for the group as a whole. You could include both policers in ACEs that match the group's traffic. The combination would affect individuals separately and the group cumulatively.

For ACEs that include both a microflow policer and an aggregate policer, 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, QoS applies a new DSCP value.

Follow these guidelines when creating policers:

- You can include a microflow policer in IP ACEs. You cannot include a microflow policer in IPX or MAC ACEs. IPX and MAC ACEs support only aggregate policers.
- By default, microflow policers do not affect bridged traffic. To enable microflow policing of bridged traffic, enter the **set qos bridged-microflow-policing** command (for more information, see the "Enabling or Disabling Microflow Policing of Bridged Traffic" section on page 43-52).
- With a Layer 3 Switching Engine II, to do any microflow policing, you must enable microflow policing of bridged traffic.
- With an MSFC, QoS does not apply microflow policers to Multilayer Switching (MLS) candidate frames (MSFC2 does not use candidate and enabler frames).
- To avoid inconsistent results, all ACEs that include the same aggregate policer must use the same ACE keyword: **trust-dscp**, **trust-ipprec**, **trust-cos**, or **dscp**. If the ACE uses the **dscp** keyword, all traffic that matches the ACE must come through ports that are configured with the same port keyword: **trust-dscp**, **trust-ipprec**, **trust-cos**, or **untrusted**. If the ACL is attached to a VLAN, you must configure all ports in the VLAN with the same port keyword.

PFC2 Policing Decisions

With a PFC2, the policing decision consists of two levels:

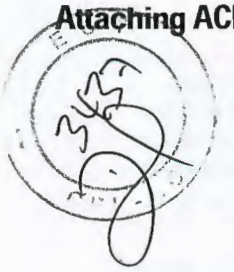
- Normal Police Level—Set if either the microflow policer or the aggregate normal rate policer returns an out-of-profile decision.
- Excess Police Level—Set if the aggregate excess rate policer returns an out-of-profile decision.

Packets are dropped if the excess rate aggregate policer returns an out-of-profile decision and the drop indication flag is set, or if the microflow policer returns an out-of-profile decision and the drop indication flag is set.

If an excess police level is set, the excess DSCP mapping is used to replace the original DSCP value with a marked-down value. If only a normal police level is set, the normal DSCP mapping is used. The excess police level has precedence for selecting mapping rules when both police levels are set because the excess police level represents the worst out-of-profile transgression.

ROSTO Nº 08/2005 - CN
CPMI - C... 0695
Fls: 0695
Doc: 3791

Attaching ACLs



You can configure each port for either port-based QoS (default) or VLAN-based QoS (see the "Enabling Port-Based or VLAN-Based QoS" section on page 43-36) and attach ACLs to the selected interface (see the "Attaching ACLs to Interfaces" section on page 43-50). You can attach up to three named ACLs, one of each type (IP, IPX, and Ethernet) to each port and VLAN.

On ports that are configured for VLAN-based QoS, you can attach named ACLs to the port's VLAN. For a trunk, you can attach named ACLs to any VLANs that are allowed on the trunk as follows:

- On a port that is configured for VLAN-based QoS, traffic that is received through the port is compared to any named ACLs that are attached to the port's VLAN. If you do not attach any named ACLs to the port's VLAN, or if the traffic does not match an ACE in a named ACL, QoS compares the traffic that is received through the port to the default ACLs.
- On a trunk that is configured for VLAN-based QoS, traffic that is received through the port is compared to any named ACLs that are attached to the traffic's VLAN. For traffic in VLANs that have no named ACLs attached, or if the traffic does not match an ACE in a named ACL, QoS compares the traffic to the default ACLs.

On ports that are configured for port-based QoS, you can attach named ACLs to the port as follows:

- On a port that is configured for port-based QoS, traffic that is received through the port is compared to any named ACLs that are attached to the port. If you do not attach any named ACLs to the port, or if the traffic does not match an ACE in a named ACL, QoS compares the traffic that is received through the port to the default ACLs.
- On a trunk that is configured for port-based QoS, traffic in all VLANs that are received through the port is compared to any named ACLs that are attached to the port. If you do not attach any named ACLs to the port, or if the traffic does not match an ACE in a named ACL, QoS compares the traffic that is received through the port to the default ACLs.

Final Layer 3 Switching Engine CoS and ToS Values

With a Layer 3 switching engine, QoS associates CoS and ToS values with traffic as specified by the marking rules and policers in the ACE that the traffic matches (see the "Internal DSCP Values" section on page 43-17). The associated CoS and ToS are used at the Ethernet egress port (see the "Ethernet Egress Port Scheduling, Congestion Avoidance, and Marking" section on page 43-27).

Classification and Marking with a Layer 2 Switching Engine

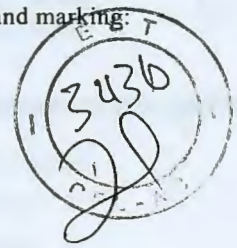
With a Layer 2 Switching Engine, QoS can classify traffic that is addressed to specified MAC address/VLAN pairs to be marked with a configured CoS value (for more information, see the "QoS Terminology" section on page 43-2 and the "Mapping a CoS Value to a Host Destination MAC Address/VLAN Pair" section on page 43-51).

Note Classification and marking with a Layer 2 Switching Engine uses Layer 2 CoS values. Classification and marking with a Layer 2 Switching Engine does not use or set Layer 3 IP precedence or DSCP values.

Ethernet Egress Port Scheduling, Congestion Avoidance, and Marking

These sections describe Ethernet egress port scheduling, congestion avoidance, and marking:

- Overview, page 43-27
- Transmit Queues, page 43-27
- Scheduling and Congestion Avoidance, page 43-28
- Marking, page 43-30



Overview

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 that is transmitted from Ethernet ports.

Note Ethernet egress port scheduling and congestion avoidance uses Layer 2 CoS values. Ethernet egress port marking writes Layer 2 CoS values, and for IP traffic, the Layer 3 ToS byte.

Transmit Queues

Enter the **show port capabilities** command to see the queue structure of a port. The command displays one of the following:

- **tx-(2q2t)** indicates two standard queues, each with two configurable tail-drop thresholds.
- **tx-(1p2q2t)** indicates one strict-priority queue and two standard queues, each with two configurable WRED-drop thresholds.
- **tx-(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).
- **tx-(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 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 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.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 0696
Doc: 3701

On **1p3q1t** ports, the transmit queue size is not configurable and is allocated equally among all queues.

On **1p2q1t** ports, the default 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.

Scheduling and Congestion Avoidance

These sections describe scheduling and congestion avoidance:

- 2q2t Ports, page 43-28
- 1p2q2t Ports, page 43-28
- 1p3q1t Ports, page 43-29
- 1p2q1t Ports, page 43-29

Note The explanations in these sections use default values. You can configure many of the parameters (for more information, see the "Configuring QoS on the Switch" section on page 43-34). 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) as follows:
  - 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) as follows:
  - 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 nonconfigurable 100 percent tail-drop threshold and a configurable WRED-drop threshold (see the "1p3q1t Transmit Queues" section on page 43-59). The switch uses tail-drop thresholds for traffic carrying CoS values that are mapped only to a queue. The switch uses WRED-drop thresholds for traffic carrying CoS values that are mapped to a queue and a threshold.

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 as follows:
  - 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 by mapping a CoS value to a queue or to a queue and a threshold. The switch uses tail-drop thresholds for traffic carrying CoS values that are mapped only to a queue. The switch uses WRED-drop thresholds for traffic carrying CoS values that are mapped to a queue and a threshold. See the "1p2q1t Transmit Queues" section on page 43-60.

RQS Nº 03/2005 - CPMI - CORREIOS
0697
Fls:
Doc: 3701

Marking

When traffic is transmitted from the switch, QoS writes the ToS byte into IP traffic (Layer 3 switching engine only) and the CoS value that was used for scheduling and congestion avoidance into ISL or 802.1Q traffic (for more information, see the "Final Layer 3 Switching Engine CoS and ToS Values" section on page 43-26).

QoS Statistics Data Export

The QoS statistics data export feature generates per-port and per-aggregate policer utilization information and forwards this information in UDP packets to traffic monitoring, planning, or accounting applications. You can enable QoS statistics data export on a per-port or per-aggregate policer basis. The statistics data that is generated per port consists of counts of the input and output packets and bytes. The aggregate policer statistics consists of counts of allowed packets and counts of packets exceeding the policed rate.

The QoS statistics data collection occurs periodically at a fixed interval, but the interval at which the data is exported is configurable. QoS statistics collection is enabled by default, and the data export feature is disabled by default for all ports and all aggregate policers that are configured on the Catalyst 6500 series switch.

Note

- Per-port counter information and utilization statistics are not available for ATM ports.
- The QoS statistics data export feature is completely separate from TopN and NetFlow Data Export and does not interact with either of these features.

For information on configuring QoS statistics data export, see the "Configuring QoS Statistics Data Export" section on page 43-76.

QoS Default Configuration

Table 43-3 shows the QoS default configuration.

Table 43-3 QoS Default Configuration

Feature	Default Value
QoS enable state	Disabled **Note**—With QoS enabled and all other QoS parameters at default values, QoS sets Layer 3 DSCP to 0 and Layer 2 CoS to 0 in all traffic that is transmitted from the switch.
Port CoS value	0
IntraVLAN microflow policing	Disabled

Table 43-3 QoS Default Configuration (continued)

Feature	Default Value
CoS to internal DSCP map (internal 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 internal DSCP map (internal 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
Internal DSCP to egress CoS map (egress CoS set from internal 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
Named ACLs	None
Default ACLs	Supports per-port classification and marking, sets DSCP to 0 in traffic from untrusted ports, no policing
COPS[1] support	Disabled
RSVP support	Disabled
QoS statistics data export	Disabled
h QoS enabled	
Runtime—Port based or VLAN based	Port based
Config—Port based or VLAN based	Port based
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

ECT 3432 CPMI - CORREIOS
RQS Nº 03/2005 - CN
CPMI - CORREIOS
0698
Fls: 3701
Doc:

Table 43-3 QoS Default Configuration (continued)

Feature	Default Value
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**.
1p1q4t/1p2q2t port receive and transmit-queue CoS value/drop-threshold mapping and threshold percentages	• Strict-priority receive queue 1 and strict-priority transmit queue 1: 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 – 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 6 and 7 – Transmit queue low and high WRED-drop thresholds: 70% and 100%

ECT 3430 CPLAN

Table 43-3 QoS Default Configuration (continued)

Feature	Default Value
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
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

ROS Nº 03/2005 - CN
CPMI - CORR 43-33
0699
Fls: 3701
Doc:

Table 43-3 QoS Default Configuration (continued)

Feature	Default Value
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
With QoS disabled	
Runtime—Port based or VLAN based	VLAN based
Config—Port based or VLAN based	Port based
Port trust state	**trust-cos** (Layer 2 switching engine) **trust-dscp** (Layer 3 switching engine)
Receive-queue drop-threshold percentages	All thresholds set to 100%
Transmit-queue drop-threshold percentages	All thresholds set to 100%
Transmit-queue low-priority/high-priority bandwidth allocation ratio	255:1
Transmit-queue size ratio	• Low priority: 100% • High priority: Not used
CoS value/drop-threshold mapping	Receive-drop threshold 1 and transmit-queue 1/drop threshold 1: CoS 0–7

1. COPS = Common Open Policy Service

Configuring QoS on the Switch

These sections describe how to configure QoS on the Catalyst 6500 series switches:

- Enabling QoS, page 43-35
- Enabling Port-Based or VLAN-Based QoS, page 43-36
- Configuring the Trust State of a Port, page 43-36
- Configuring the CoS Value for a Port, page 43-37
- Creating Policers, page 43-38
- Deleting Policers, page 43-40
- Creating or Modifying ACLs, page 43-41
- Attaching ACLs to Interfaces, page 43-50
- Detaching ACLs from Interfaces, page 43-50

- Mapping a CoS Value to a Host Destination MAC Address/VLAN Pair, page 43-51
- Deleting a CoS Value to a Host Destination MAC Address/VLAN Pair, page 43-51
- Enabling or Disabling Microflow Policing of Bridged Traffic, page 43-52
- Configuring Standard Receive-Queue Tail-Drop Thresholds, page 43-52
- Configuring 2q2t Port Standard Transmit-Queue Tail-Drop Thresholds, page 43-53
- Configuring Standard Queue WRED-Drop Thresholds, page 43-53
- Allocating Bandwidth Between Standard Transmit Queues, page 43-55
- Configuring the Receive-Queue Size Ratio, page 43-56
- Configuring the Transmit-Queue Size Ratio, page 43-56
- Mapping CoS Values to Drop Thresholds, page 43-56
- Configuring DSCP Value Maps, page 43-61
- Displaying QoS Information, page 43-64
- Displaying QoS Statistics, page 43-65
- Reverting to QoS Defaults, page 43-66
- Disabling QoS, page 43-66
- Configuring COPS Support, page 43-66
- Configuring RSVP Support, page 43-72
- Configuring QoS Statistics Data Export, page 43-76

Note Some QoS **show** commands support the **config** and **runtime** keywords. Use the **runtime** keyword to display the QoS values that are currently programmed into the hardware. When you disable QoS, the display with the **runtime** keyword is "QoS is disabled." Use the **config** keyword to display values from commands that have been entered but which may not currently be programmed into the hardware (for example, locally configured QoS values that are currently not used because COPS has been selected as the QoS policy source or QoS values that are configured when QoS is disabled).

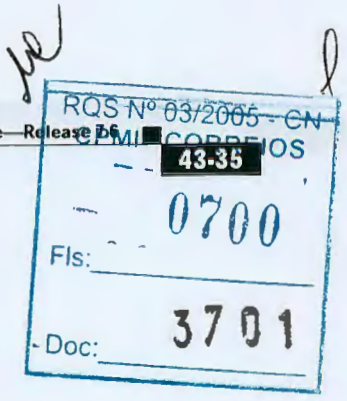
Enabling QoS

To enable QoS, perform this task in privileged mode:

Task	Command
Enable QoS on the switch.	**set qos {enable | disable}**

This example shows how to enable QoS:

```
Console> (enable) set qos enable
QoS is enabled.
Console> (enable)
```



Enabling Port-Based or VLAN-Based QoS

Note The commands in this section are not supported with a Layer 2 Switching Engine.

By default, QoS uses ACLs that are attached to ports. On a per-port basis, you can configure QoS to use ACLs that are attached to a VLAN. To enable VLAN-based QoS on a port, perform this task in privileged mode:

	Task	Command
Step 1	Enable VLAN-based QoS on a port.	**set port qos** *mod/port* {**port-based** | **vlan-based**}
Step 2	Verify the configuration.	**show port qos** *mod/port*

For more information, see the "Attaching ACLs" section on page 43-26.

This example shows how to enable VLAN-based QoS on a port:

```
Console> (enable) set port qos 1/1-2 vlan-based
Hardware programming in progress...
QoS interface is set to vlan-based for ports 1/1-2.
Console> (enable)
```

Changing a port from port-based to VLAN-based QoS detaches all ACLs from the port. Any ACLs that are attached to the VLAN apply to the port immediately (for more information, see the "Attaching ACLs to Interfaces" section on page 43-50).

Configuring the Trust State of a Port

This command configures the trust state of a port (for more information, see the "Ethernet Ingress Port Marking, Scheduling, Congestion Avoidance, and Classification" section on page 43-10). By default, all ports are untrusted.

To configure the trust state of a port, perform this task in privileged mode:

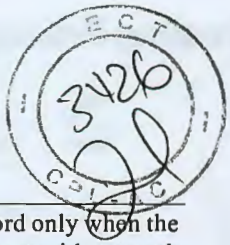
	Task	Command
Step 1	Configure the trust state of a port.	**set port qos trust** {**untrusted** | **trust-cos** | **trust-ipprec** | **trust-dscp**}
Step 2	Verify the configuration.	**show port qos**

Note the following syntax guidelines when configuring the trust state of a port:

- The **trust-ipprec** and **trust-dscp** keywords are supported only with a Layer 3 switching engine.
- **1q4t** ports (except Gigabit Ethernet) do not support the **trust-ipprec** and **trust-dscp** port keywords. You must configure a **trust-ipprec** or **trust-dscp** ACL that matches the ingress traffic to apply the **trust-ipprec** or **trust-dscp** trust state.
- On **1q4t** ports (except Gigabit Ethernet), the **trust-cos** port keyword displays an error message, activates receive-queue drop thresholds, and—as indicated by the error message—does not apply the **trust-cos** trust state to traffic. You must configure a **trust-cos** ACL that matches the ingress traffic to apply the **trust-cos** trust state.

This example shows how to configure port 1/1 with the **trust-cos** keyword:

```
Console> (enable) set port qos 1/1 trust trust-cos
Port 1/1 qos set to trust-cos
Console> (enable)
```



Note Only ISL or 802.1Q frames carry CoS values. Configure ports with the **trust-cos** keyword only when the received traffic is ISL or 802.1Q frames carrying CoS values that you know to be consistent with network policy.

Configuring the CoS Value for a Port

Note Whether or not QoS uses the CoS value that is applied with the **set port qos ...cos** command depends on the trust state of the port and the trust state of the traffic that is received through the port. The **set port qos ... cos** command does not configure the trust state of the port or the trust state of the traffic that is received through the port. To use the CoS value that is applied with the **set port qos ... cos** command, configure a trust-CoS ACL that matches the ingress traffic; or for a port that receives no tagged traffic, configure the port to trust CoS.

Unmarked frames from ports that are configured as trusted and all frames from ports that are configured as untrusted are assigned the CoS value that is specified with this command.

To configure the CoS value for a port, perform this task in privileged mode:

	Task	Command
Step 1	Configure the CoS value for a port.	**set port qos cos** *cos_value*
Step 2	Verify the configuration.	**show port qos**

This example shows how to configure the port CoS value to 3 for port 1/1:

```
Console> (enable) set port qos 1/1 cos 3
Port 1/1 qos cos set to 3
Console> (enable)
```

To revert to the default CoS value for a port, perform this task in privileged mode:

	Task	Command
Step 1	Revert to the default CoS value for a port.	**clear port qos cos**
Step 2	Verify the configuration.	**show port qos**

This example shows how to revert to the default CoS value for port 1/1:

```
Console> (enable) clear port qos 1/1 cos
Port 1/1 qos cos setting cleared.
Console> (enable)
```


CPMI CORREIOS 43-37
0701
Fls: 3701
Doc:

Creating Policers

Note The commands in this section are not supported with a Layer 2 Switching Engine.

To create a policer, perform this task in privileged mode:

	Task	Command
Step 1	Create a policer.	**set qos policer microflow** *microflow_name* {**rate** *rate*} {**burst** *burst_value*} {**drop** | **policed-dscp**} With PFC or PFC2: **set qos policer aggregate** *aggregate_name* {**rate** *rate*} {**burst** *burst_value*} {**drop** | **policed-dscp**} With PFC2: **set qos policer aggregate** *aggregate_name* {**rate** *rate*} **policed-dscp** {**erate** *erate_value*} {**drop** | **policed-dscp**} **burst** *burst_value* [**eburst** *eburst_value*]
Step 2	Verify the configuration.	**show qos policer** {**config** | **runtime**} {**microflow** | **aggregate** | **all**}

For more information, see the "Policers" section on page 43-24 and the"PFC2 Policing Decisions" section on page 43-25.

The *policer_name* parameter can be up to 31 characters long, is case sensitive, and may include a–z, A–Z, 0–9, the dash character (-), the underscore character (_), and the period character (.). Policer names must start with an alphabetic character (not a digit) and must be unique across all microflow and aggregate policers. You cannot use keywords from any command as a policer name.

The valid values for the *rate* and *erate* parameters are 32 Kbps (entered as 32) to 32 Gbps (entered as 32000000); or to classify all traffic as out of profile, set the *rate* parameter to zero (0). Set the *erate* parameter to a higher value than the *rate* parameter. The PFC1 and PFC2 have the following hardware granularity for rate values:

Rate Value Range	Granularity	Rate Value Range	Granularity
1 to 1024 (1 Mbs)	32768 (32 K)	65537 to 131072 (128 Mbs)	4194304 (4 M)
1025 to 2048 (2 Mbs)	65536 (64 K)	131073 to 262144 (256 Mbs)	8388608 (8 M)
2049 to 4096 (4 Mbs)	131072 (128 K)	262145 to 524288 (512 Mbs)	16777216 (16 M)
4097 to 8192 (8 Mbs)	262144 (256 K)	524289 to 1048576 (1 Gps)	33554432 (32 M)
8193 to 16384 (16 Mbs)	524288 (512 K)	1048577 to 2097152 (2 Gps)	67108864 (64 M)
16385 to 32768 (32 Mbs)	1048576 (1 M)	2097153 to 4194304 (4 Gps)	134217728 (128 M)
32769 to 65536 (64 Mbs)	2097152 (2 M)	4194305 to 8000000 (8 Gps)	268435456 (256 M)

Within each range, QoS programs the hardware with rate values that are multiples of the granularity values.

ECT 3424 CPI AC

The valid values for the *burst* and *eburst* parameters are 1 Kb (entered as 1) to 256 Mb (entered as 256000). When configuring *burst* and *eburst* parameters, note the following:

- The **burst** keyword, the *burst_value* parameter, the optional **eburst** keyword, and the *eburst_value* parameter set the token bucket sizes. To sustain a specific rate, set the token bucket size to be at least the *rate* divided by 4000, because tokens are removed from the bucket every 1/4000th of a second (0.25 ms) and the bucket needs to be at least as large as the burst size to sustain the specified rate.
- If you do not enter the **eburst** keyword and the *eburst_value* parameter, QoS sets both token buckets to the size that is configured with the **burst** keyword and the *burst_value* parameter.
- Because any packet larger than the burst size is considered an out-of-profile packet, make sure that the burst size is greater than or equal to the largest packet size being policed.
- QoS programs the hardware with values that are multiples of 32K (32,768), not with the specific value entered.

Enter either the **drop** keyword to cause all out-of-profile packets to be dropped or the **policed-dscp** keyword to cause all out-of-profile packets with the normal rate to be marked down as specified in the normal markdown DSCP map (for more information, see the "Mapping DSCP Markdown Values" section on page 43-63).

This example shows how to create a microflow policer with a 1-Mbps rate limit and a 10-Mb burst limit that marks down out-of-profile traffic:

```
Console> (enable) set qos policer microflow my-micro rate 1000 burst 10000 policed-dscp
Hardware programming in progress...
QoS policer for microflow my-micro created successfully.
Console> (enable)
```

For PFC2, this example shows how to create an aggregate excess rate policer with a 64-Kbps rate limit and a 128-Kb burst limit that drops traffic exceeding these values:

```
Console> (enable) set qos policer aggregate test rate 64 burst 128 drop
QoS policer for aggregate test created successfully.
Console> (enable) show qos policer config aggregate test
QoS aggregate policers:
QoS aggregate policers:
Aggregate name                 Normal rate (kbps) Burst size (kb) Normal action
------------------------------ ------------------ --------------- -------------
test                                           64             128 policed-dscp
                               Excess rate (kbps) Burst size (kb) Excess action
                               ------------------ --------------- -------------
                                               64             128 drop
                               ACL attached
                               -----------------------------------

Console> (enable)
```

For PFC2, this example shows how to create an aggregate excess rate policer with a 64-Kbps rate limit and a 100-Kb burst limit that will cause all out-of-profile packets to be marked down as specified in the normal markdown DSCP map:

```
Console> (enable) set qos policer aggregate test2 rate 64 burst 100 policed-dscp
QoS policer for aggregate test2 created successfully.
Console> (enable) show qos policer config aggregate test2
QoS aggregate policers:
```


RGS N° 08/2005 - CN
CPMI - CORREIOS
43.39
0702
Fls:
Doc: 3701

```
Aggregate name                   Normal rate (kbps)  Burst size (kb) Normal action
-------------------------------- ------------------  --------------- ------------
test2                                            64             100  policed-dscp
                                 Excess rate (kbps)  Burst size (kb) Excess action
                                 ------------------  --------------- ---------------
                                            8000000             100  policed-dscp
                                 ACL attached
                                 ------------------------------------

Console> (enable)
```

For PFC2, this example shows how to create an aggregate excess rate policer with a 64-Kbps rate limit and a 128-Kb burst limit that will cause traffic that exceeds the normal rate of 64 Kbps and a burst size of 96 Kb to be marked down as specified in the normal markdown DSCP map, and traffic that exceeds 128 Kbps and a burst size of 96 Kb to be dropped:

```
Console> (enable) set qos policer aggregate test3 rate 64 policed-dscp erate 128 drop
burst 96
QoS policer for aggregate test3 created successfully.
Console> (enable) show qos policer config aggregate test3
QoS aggregate policers:
Aggregate name                   Normal rate (kbps)  Burst size (kb) Normal action
-------------------------------- ------------------  --------------- ------------
test3                                            64              96  policed-dscp
                                 Excess rate (kbps)  Burst size (kb) Excess action
                                 ------------------  --------------- ---------------
                                               128              96  drop
                                 ACL attached
                                 ------------------------------------

Console> (enable)
```

Deleting Policers

Note You can only delete policers if they are not attached to any interfaces (for more information, see the "Detaching ACLs from Interfaces" section on page 43-50).

To delete one or all policers, perform this task in privileged mode:

	Task	Command
Step 1	Delete one or all policers.	**clear qos policer** {**microflow** | **aggregate**} {*policer_name* | **all**}
Step 2	Verify the configuration.	**show qos policer** {**config** | **runtime**} {**microflow** | **aggregate** | **all**}

This example shows how to delete the microflow policer named my_micro:

```
Console> (enable) clear qos policer microflow my_micro
my_micro QoS microflow policer cleared.
Console> (enable)
```

Creating or Modifying ACLs

Note The commands in this section are not supported with a Layer 2 Switching Engine.

These sections describe ACL creation and modification:

- ACL Names, page 43-41
- ACE Name, Marking Rule, Policing, and Filtering Syntax, page 43-41
- Named IP ACLs, page 43-42
- Modifying the Default IP ACL, page 43-46
- Creating or Modifying Named IPX ACLs, page 43-46
- Creating or Modifying Named MAC ACLs, page 43-47
- Creating or Modifying the Default IPX and MAC ACLs, page 43-48
- Deleting Named ACLs, page 43-48
- Reverting to Default Values in Default ACLs, page 43-48
- Discarding Uncommitted ACLs, page 43-49
- Committing ACLs, page 43-49

ACL Names

ACL names can be up to 31 characters long, are case sensitive, and may include a–z, A–Z, 0–9, the dash character (-), the underscore character (_), and the period character (.). ACL names must start with an alphabetic character and must be unique across all QoS ACLs of all types. You cannot use keywords from any command as an ACL name.

ACE Name, Marking Rule, Policing, and Filtering Syntax

ACE command syntax is organized as follows:
ACL_command ACL_type_and_name marking_rule policing_rule filtering

For example, in an IP ACE, the command syntax is as follows:

set qos acl ip *acl_name* {**dscp** *dscp_value* | **trust-cos** | **trust-ipprec** | **trust-dscp**} [**microflow** *microflow_name*] [**aggregate** *aggregate_name*] *src_ip_spec* [**precedence** *precedence* | **dscp-field** *dscp*] [**before** *editbuffer_index* | **modify** *editbuffer_index*]

- **set qos acl ip** *acl_name*—Creates a named ACL of the specified type or adds the ACE to the ACL if it already exists. See the "ACL Names" section on page 43-41.
- {**dscp** *dscp_value* | **trust-cos** | **trust-ipprec** | **trust-dscp**}—Selects a marking rule. See the "Marking Rules" section on page 43-23.
- [**microflow** *microflow_name*] [**aggregate** *aggregate_name*]—Optionally configures policing in the ACE. See the "Policers" section on page 43-24.
- *src_ip_spec* [**precedence** *precedence* | **dscp-field** *dscp*]—The rest of the parameters, except the **editbuffer** keywords, configure filtering.

RQS N° 43-41 CN
CPMI - CORREIOS
Fls: 0703
Doc: 3701

Named IP ACLs

These sections describe creating or modifying IP ACLs:

- Source and Destination IP Addresses and Masks, page 43-42
- Port Operator Parameters, page 43-42
- Precedence Parameter Options, page 43-42
- IP ACEs for TCP Traffic, page 43-43
- IP ACEs for UDP Traffic, page 43-43
- IP ACEs for ICMP Traffic, page 43-44
- IP ACEs for IGMP Traffic, page 43-44
- IP ACLs for Other Layer 4 Protocols, page 43-45
- IP ACEs for Any IP Traffic, page 43-45

Source and Destination IP Addresses and Masks

In IP ACEs, specify the source and destination IP addresses and masks (represented by the *src_ip_spec* and *dest_ip_spec* parameters in the following sections) in the form *ip_address mask*. The mask is mandatory. Use one bits, which need not be contiguous, where you want wildcards.

Use any of the following formats for the address and mask:

- Four-part dotted-decimal 32-bit values
- The keyword **any** as an abbreviation for a wildcard address and wildcard mask of 0.0.0.0 255.255.255.255
- The abbreviation **host** *ip_address* for an address and wildcard mask of *ip_address* 0.0.0.0

Port Operator Parameters

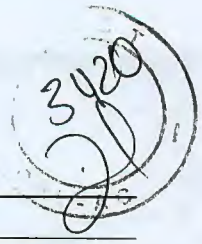
In IP ACEs, the *operator* parameter can be one of the following:

- **lt** (less than)
- **gt** (greater than)
- **eq** (equal)
- **neq** (not equal)
- **range** (with a pair of port parameters)

See the "Layer 4 Operations Configuration Guidelines" section on page 16-23 for restrictions that apply to QoS ACLs.

Precedence Parameter Options

For *precedence* parameter keyword options in IP ACEs, see the "IP ACE Layer 3 Classification Criteria" section on page 43-18.



IP ACEs for TCP Traffic

To create or modify an IP ACE for TCP traffic, perform this task in privileged mode:

	Task	Command
Step 1	Create or modify an IP ACE for TCP traffic.	**set qos acl ip** {*acl_name*} {{**dscp** *dscp_value*} | **trust-cos** | **trust-ipprec** | **trust-dscp**} [**microflow** *microflow_name*] [**aggregate** *aggregate_name*] **tcp** {*src_ip_spec*} [{*operator*} {*port*} [*port*]] {*dest_ip_spec*} [{*operator*} {*port*} [*port*]] [**established**] [**precedence** *precedence_value* | **dscp-field** *dscp*] [**before** *editbuffer_index* | **modify** *editbuffer_index*]
Step 2	Verify the configuration.	**show qos acl info** {**acl_name** | **all**} **editbuffer** [*editbuffer_index*]

For *port* parameter keyword options, see the "IP ACE Layer 4 TCP Classification Criteria" section on page 43-19.

The **established** keyword matches traffic with the ACK or RST bits set.

This example shows how to create an IP ACE for TCP traffic:

```
Console> (enable) set qos acl ip my_IPacl trust-ipprec microflow my-micro aggregate my-agg
tcp any any
my_IPacl editbuffer modified. Use 'commit' command to apply changes.
Console> (enable)
```

IP ACEs for UDP Traffic

To create or modify an IP ACE for UDP traffic, perform this task in privileged mode:

	Task	Command
Step 1	Create or modify an IP ACE for UDP traffic.	**set qos acl ip** {*acl_name*} {{**dscp** *dscp_value*} | **trust-cos** | **trust-ipprec** | **trust-dscp**} [**microflow** *microflow_name*] [**aggregate** *aggregate_name*] **udp** {*src_ip_spec*} [{*operator*} {*port*} [*port*]] {*dest_ip_spec*} [{*operator*} {*port*} [*port*]] [**precedence** *precedence_value* | **dscp-field** *dscp*] [**before** *editbuffer_index* | **modify** *editbuffer_index*]
Step 2	Verify the configuration.	**show qos acl info** {**acl_name** | **all**} **editbuffer** [*editbuffer_index*]

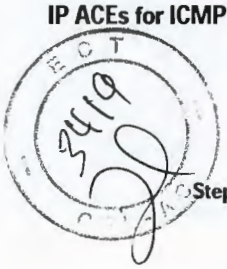
For *port* parameter keyword options, see the "IP ACE Layer 4 UDP Classification Criteria" section on page 43-20.

This example shows how to create an IP ACE for UDP traffic:

```
Console> (enable) set qos acl ip my_IPacl trust-ipprec microflow my-micro aggregate my-agg
udp any any
my_IPacl editbuffer modified. Use 'commit' command to apply changes.
Console> (enable)
```


ROS Nº 03/2005 - CN
CPMI - C 43-43 DS
0704
Fls:
Doc: 3701

IP ACEs for ICMP Traffic



To create or modify an IP ACE for ICMP traffic, perform this task in privileged mode:

	Task	Command
Step 1	Create or modify an IP ACE for ICMP traffic.	**set qos acl ip** *acl_name* {**dscp** *dscp* | **trust-cos** | **trust-ipprec** | **trust-dscp**} [**microflow** *microflow_name*] [**aggregate** *aggregate_name*] **icmp** *src_ip_spec dest_ip_spec* [*icmp_type* [*icmp_code*] | *icmp_message*] [**precedence** *precedence* | **dscp-field** *dscp*] [**before** *editbuffer_index* | **modify** *editbuffer_index*]
Step 2	Verify the configuration.	**show qos acl info** {**acl_name** | **all**} **editbuffer** [*editbuffer_index*]

For *icmp_code* and *icmp_type* parameter keyword options, see the "IP ACE Layer 4 ICMP Classification Criteria" section on page 43-20.

This example shows how to create an IP ACE for ICMP *echo* traffic:

```
Console> (enable) set qos acl ip my_IPacl trust-ipprec microflow my-micro aggregate my-agg
icmp any any echo
my_IPacl editbuffer modified. Use 'commit' command to apply changes.
Console> (enable)
```

IP ACEs for IGMP Traffic

Note QoS does not support IGMP traffic when IGMP snooping is enabled.

To create or modify an IP ACE for IGMP traffic, perform this task in privileged mode:

	Task	Command
Step 1	Create or modify an IP ACE for IGMP traffic.	**set qos acl ip** *acl_name* {**dscp** *dscp_value* | **trust-cos** | **trust-ipprec** | **trust-dscp**} [**microflow** *microflow_name*] [**aggregate** *aggregate_name*] **igmp** *src_ip_spec dest_ip_spec* [*igmp_type*] [**precedence** *precedence_value* | **dscp-field** *dscp*] [**before** *editbuffer_index* | **modify** *editbuffer_index*]
Step 2	Verify the configuration.	**show qos acl info** {**acl_name** | **all**} **editbuffer** [*editbuffer_index*]

3418

For *igmp_type* parameter keyword options, see the "IP ACE Layer 4 IGMP Classification Criteria" section on page 43-21.

This example shows how to create an IP ACE for IGMP Protocol Independent Multicast (PIM) traffic:

```
Console> (enable) set qos acl ip my_IPacl trust-ipprec microflow my-micro aggregate my-agg
igmp any any pim
my_IPacl editbuffer modified. Use 'commit' command to apply changes.
Console> (enable)
```

IP ACLs for Other Layer 4 Protocols

To create or modify a named IP ACL with additional parameters that match all Layer 4 protocols, perform this task in privileged mode:

	Task	Command
Step 1	Create or modify an IP ACE.	**set qos acl ip** *acl_name* {**dscp** *dscp_value* | **trust-cos** | **trust-ipprec** | **trust-dscp**} [**microflow** *microflow_name*] [**aggregate** *aggregate_name*] *protocol src_ip_spec dest_ip_spec* [**precedence** *precedence_value* | **dscp-field** *dscp*] [**before** *editbuffer_index* | **modify** *editbuffer_index*]
Step 2	Verify the configuration.	**show qos acl info** {**acl_name** | **all**} **editbuffer** [*editbuffer_index*]

For *protocol* parameter keyword options, see the "IP ACE Layer 4 Protocol Classification Criteria" section on page 43-19.

This example shows how to create an IP ACE for IPINIP traffic:

```
Console> (enable) set qos acl ip my_IPacl trust-ipprec microflow my-micro aggregate my-agg
ipinip any any
my_IPacl editbuffer modified. Use 'commit' command to apply changes.
Console> (enable)
```

IP ACEs for Any IP Traffic

To create or modify an IP ACE that matches all IP traffic, perform this task in privileged mode:

	Task	Command
Step 1	Create or modify an IP ACE.	**set qos acl ip** *acl_name* {**dscp** *dscp* | **trust-cos** | **trust-ipprec** | **trust-dscp**} [**microflow** *microflow_name*] [**aggregate** *aggregate_name*] *src_ip_spec* [**precedence** *precedence* | **dscp-field** *dscp*] [**before** *editbuffer_index* | **modify** *editbuffer_index*]
Step 2	Verify the configuration.	**show qos acl info** {**acl_name** | **all**} **editbuffer** [*editbuffer_index*]

CPMI - CORREIOS
0705
Fls:
Doc: 3701

This example shows how to create an IP ACE:

```
Console> (enable) set qos acl ip my_IPacl trust-ipprec microflow my-micro aggregate my-agg
any
my_IPacl editbuffer modified. Use 'commit' command to apply changes.
Console> (enable)
```

Modifying the Default IP ACL

To modify the default IP ACL, perform this task in privileged mode:

	Task	Command
Step 1	Modify the default IP ACL.	**set qos acl default-action ip** {**dscp** *dscp* | **trust-cos** | **trust-ipprec** | **trust-dscp**} [**microflow** *microflow_name*] [**aggregate** *aggregate_name*]
Step 2	Verify the configuration.	**show qos acl info default-action** {**ip** | **ipx** | **mac** | **all**}

For more information, see the "Default ACLs" section on page 43-22.

This example shows how to modify the default IP ACL:

```
Console> (enable) set qos acl default-action ip dscp 5 microflow my-micro aggregate my-agg
QoS default-action for IP ACL is set successfully.
Console> (enable)
```

Creating or Modifying Named IPX ACLs

To create or modify a named IPX ACL, perform this task in privileged mode:

	Task	Command
Step 1	Create or modify a named IPX ACL.	With PFC: **set qos acl ipx** *acl_name* {**dscp** *dscp_value* | **trust-cos**} [**aggregate** *aggregate_name*] *protocol src_net* [*dest_net*[*.dest_node*] [[*dest_net_mask*] *.dest_node_mask*]] [**before** *editbuffer_index* | **modify** *editbuffer_index*] With PFC2: **set qos acl ipx** *acl_name* **aggregate** *aggregate_name protocol src_net* [*dest_net*[*.dest_node*] [[*dest_net_mask*] *.dest_node_mask*]] [**before** *editbuffer_index* | **modify** *editbuffer_index*]
Step 2	Verify the configuration.	**show qos acl info** {**acl_name** | **all**} **editbuffer** [*editbuffer_index*]

The *protocol* parameter can be specified numerically (0–255) or with these keywords: **any**, **ncp** (17), **netbios** (20), **rip** (1), **sap** (4), or **spx** (5).

The *src_net* and *dest_net* parameters are IPX network numbers, entered as up to 8 hexadecimal digits in the range 1 to FFFFFFFE (-1 matches any network number). You do not need to enter leading zeros.

If you specify an IPX destination network, IPX ACEs support the following optional parameters:

- An IPX destination network mask, entered as up to 8 hexadecimal digits in the range 1 to FFFFFFFE (-1 matches any network number). Use one bits, which need not be contiguous, where you want wildcards.
- An IPX destination node, entered as 12 hexadecimal digits (48 bits), formatted as a dotted triplet of four-digit hexadecimal digits each (xxxx.xxxx.xxxx).
- If you specify an IPX destination node, IPX ACEs support an IPX destination node mask, entered as 12 hexadecimal digits (48 bits), formatted as a dotted triplet of four-digit hexadecimal digits each (xxxx.xxxx.xxxx). Use one bits, which need not be contiguous, where you want wildcards.

This example shows how to create an IPX ACE:

```
Console> (enable) set qos acl ipx my_IPXacl trust-cos aggregate my-agg -1
my_IPXacl editbuffer modified. Use 'commit' command to apply changes.
Console> (enable)
```

Creating or Modifying Named MAC ACLs

To create or modify a named MAC ACL, perform this task in privileged mode:

	Task	Command
Step 1	Create or modify a named MAC ACL.	With PFC: **set qos acl mac** *acl_name* {**dscp** *dscp_value* | **trust-cos**} [**aggregate** *aggregate_name*] *src_mac_spec dest_mac_spec* [*ethertype*] [**before** *editbuffer_index* | **modify** *editbuffer_index*] With PFC2: **set qos acl mac** *acl_name* **aggregate** *aggregate_name src_mac_spec dest_mac_spec* [*ethertype*] [**before** *editbuffer_index* | **modify** *editbuffer_index*]
Step 2	Verify the configuration.	**show qos acl info** {**acl_name** | **all**} **editbuffer** [*editbuffer_index*]

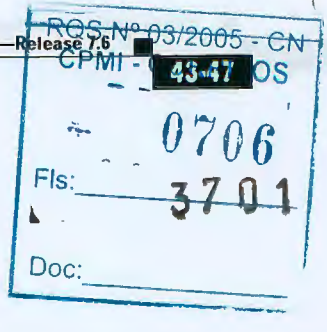
Enter the *src_mac_spec* and *dest_mac_spec* parameters as a MAC address and a mask. Each parameter is 12 hexadecimal digits (48 bits), formatted as dash-separated pairs. Use one bits, which need not be contiguous, where you want wildcards. Use the **any** keyword for a MAC address and mask of 0-0-0-0-0-0 ff-ff-ff-ff-ff-ff. Use the **host** keyword with a MAC address to specify an all-zero mask (*mac_address* 0-0-0-0-0-0).

Enter the *ethertype* parameter as 4 hexadecimal digits (16 bits) prefaced with **0x** (for example, 0x0600) or as a keyword (see the "MAC ACE Layer 2 Classification Criteria" section on page 43-22).

This example shows how to create a MAC ACE:

```
Console> (enable) set qos acl mac my_MACacl trust-cos aggregate my-agg any any
my_MACacl editbuffer modified. Use 'commit' command to apply changes.
Console> (enable)
```

Note QoS MAC ACLs that do not include an ethertype parameter match traffic with any value in the ethertype field, which allows MAC-level QoS to be applied to any traffic except IP and IPX.



Creating or Modifying the Default IPX and MAC ACLs

To create or modify the default IPX or MAC ACL, perform this task in privileged mode:

	Task	Command
Step 1	Create or modify the default IPX or MAC ACL.	With PFC: **set qos acl default-action {ipx | mac} {dscp** *dscp* **| trust-cos} [aggregate** *aggregate_name*] With PFC2: **set qos acl default-action {ipx | mac} aggregate** *aggregate_name*
Step 2	Verify the configuration.	**show qos acl info default-action {ip | ipx | mac | all}**

For more information, see the "Default ACLs" section on page 43-22.

This example shows how to modify the default IPX ACL:

```
Console> (enable) set qos acl default-action ipx dscp 5 aggregate my-agg
QoS default-action for IPX ACL is set successfully.
Console> (enable)
```

Note IPX and MAC ACLs do not support microflow policers.

Deleting Named ACLs

To delete a named ACL, perform this task in privileged mode:

	Task	Command
Step 1	Delete a named ACL.	**clear qos acl** *acl_name* [*editbuffer_index*]
Step 2	Verify the configuration.	**show qos acl info** {*acl_name* | **all**}

This example shows how to delete the ACL named icmp_acl:

```
Console> (enable) clear qos acl icmp_acl 1
ACL icmp_acl ACE# 1 is deleted.
icmp_acl editbuffer modified. Use 'commit' command to apply changes.
Console> (enable)
```

Reverting to Default Values in Default ACLs

To revert to the default values for a default ACL, perform this task in privileged mode:

	Task	Command
Step 1	Revert to the default values for a default ACL.	**clear qos acl default-action {ip | ipx | mac}**
Step 2	Verify the configuration.	**show qos acl info default-action {ip | ipx | mac | all}**

This example shows how to revert to the default values for the default IP ACL:

```
Console> (enable) clear qos acl default-action ip
Hardware programming in progress...
QoS default-action for IP ACL is restored to default setting.
Console> (enable)
```

Discarding Uncommitted ACLs

To discard an uncommitted new ACL or uncommitted changes to an existing ACL, perform this task in privileged mode:

	Task	Command
Step 1	Discard an uncommitted ACL.	**rollback qos acl** {*acl_name* | **all**}
Step 2	If you discarded changes to an existing ACL, verify the configuration.	**show qos acl info** {*acl_name* | **all**}

This example shows how to discard an uncommitted ACL named my_acl:

```
Console> (enable) rollback qos acl my_acl
Rollback for QoS ACL my_acl is successful.
Console> (enable)
```

Note Changes to the default ACLs take effect immediately and cannot be discarded.

Committing ACLs

When you create, change, or delete a named ACL, the changes exist temporarily in an edit buffer in memory. To commit the ACL so that it can be used, perform this task in privileged mode:

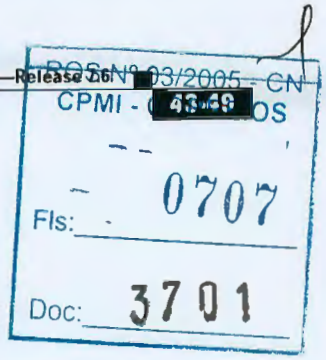
	Task	Command
Step 1	Commit an ACL.	**commit qos acl** *acl_name*
Step 2	Verify the configuration.	**show config qos acl** {*acl_name* | **all**}

This example shows how to commit an ACL named my_acl:

```
Console> (enable) commit qos acl my_acl
Hardware programming in progress...
ACL my_acl is committed to hardware.
Console> (enable)
```

Note When you commit an ACL that has already been attached to interfaces, the new values go into effect immediately. Changes to the default ACLs do not need to be committed.

See the "Configuring and Storing VACLs and QoS ACLs in Flash Memory" section on page 16-55 for information about where QoS ACLs are stored.



Attaching ACLs to Interfaces

Note The commands in this section are not supported with a Layer 2 Switching Engine.

You can attach one ACL of each type to each VLAN and to each port that is configured for port-based QoS. You cannot attach ACLs to a port that is configured for VLAN-based QoS (for more information, see the "Enabling Port-Based or VLAN-Based QoS" section on page 43-36). When an ACL of a particular type (IP, IPX, or Ethernet) is already attached to an interface, attaching a different ACL of the same type detaches the previous ACL.

To attach an ACL to a port or a VLAN, perform this task in privileged mode:

	Task	Command
Step 1	Attach an ACL to an interface.	**set qos acl map** *acl_name* {*mod/port* | *vlan*}
Step 2	Verify the configuration.	**show qos acl map** {**config** | **runtime**} {*acl_name* | *mod/port* | *vlan* | **all**}

This example shows how to attach an ACL named my_acl to port 2/1:

```
Console> (enable) set qos acl map my_acl 2/1
Hardware programming in progress...
ACL my_acl is attached to port 2/1.
Console> (enable)
```

This example shows how to attach an ACL named my_acl to VLAN 4:

```
Console> (enable) set qos acl map my_acl 4
Hardware programming in progress...
ACL my_acl is attached to vlan 4.
Console> (enable)
```

Note The default ACLs do not need to be attached to any interfaces.

Detaching ACLs from Interfaces

Note The commands in this section are not supported with a Layer 2 Switching Engine.

To detach an ACL from a port or a VLAN, perform this task in privileged mode:

	Task	Command
Step 1	Detach an ACL from an interface.	**clear qos acl map** *acl_name* {*mod/port* | *vlan* | **all**}
Step 2	Verify the configuration.	**show qos acl map** {**config** | **runtime**} {*acl_name* | *mod/port* | *vlan* | **all**}

This example shows how to detach an ACL named my_acl from port 2/1:

```
Console> (enable) clear qos acl map my_acl 2/1
Hardware programming in progress...
ACL my_acl is detached from port 2/1.
Console> (enable)
```

This example shows how to detach an ACL named my_acl from VLAN 4:

```
Console> (enable) clear qos acl map my_acl 4
Hardware programming in progress...
ACL my_acl is detached from vlan 4.
Console> (enable)
```

Note The default ACLs cannot be detached from any interfaces.

Mapping a CoS Value to a Host Destination MAC Address/VLAN Pair

Note QoS only supports this command with a Layer 2 Switching Engine.

To map a CoS value to all frames that are destined for a particular host destination MAC address and VLAN number value pair, perform this task in privileged mode:

	Task	Command
Step 1	Map a CoS value to a host destination MAC address/VLAN pair.	**set qos mac-cos** *dest_mac VLAN cos_value*
Step 2	Verify the configuration.	**show qos mac-cos** {*dest_mac* [*vlan*] | **all**}

This example shows how to map CoS 2 to a destination MAC address and VLAN 525:

```
Console> (enable) set qos mac-cos 00-40-0b-30-03-48 525 2
CoS 2 is assigned to 00-40-0b-30-03-48 vlan 525.
Console> (enable)
```

Deleting a CoS Value to a Host Destination MAC Address/VLAN Pair

Note QoS only supports this command with a Layer 2 Switching Engine.

To delete a host destination MAC address and VLAN number value pair CoS assignment, perform this task in privileged mode:

	Task	Command
Step 1	Delete a host destination MAC address and VLAN number value pair CoS assignment.	**clear qos mac-cos** {*dest_mac* [*vlan*] | **all**}
Step 2	Verify the configuration.	**show qos mac-cos** {*dest_mac* [*vlan*] | **all**}

RQS Nº 03/2005 - CN
CPMI - CO
43-51
0708
Fls:
Doc: 3701

This example shows how to delete all CoS assignments to destination MAC addresses and VLANs:

```
Console> (enable) clear qos mac-cos all
All CoS to Mac/Vlan entries are cleared.
Console> (enable)
```

Enabling or Disabling Microflow Policing of Bridged Traffic

Note The commands in this section are not supported with a Layer 2 Switching Engine.

By default, microflow policers affect only Layer 3-switched traffic. To enable or disable microflow policing of bridged traffic on the switch or on specified VLANs, perform one of these tasks in privileged mode:

Task	Command
Enable microflow policing of bridged traffic on the switch or on specified VLANs.	**set qos bridged-microflow-policing** {**enable** | **disable**} *vlan*
Disable microflow policing of bridged traffic on the switch or on specified VLANs.	**set qos bridged-microflow-policing** {**enable** | **disable**} *vlan*
Verify the configuration.	**show qos bridged-microflow-policing runtime** {**config** | **runtime**} *vlan*

Note With Layer 3 Switching Engine II, to do any microflow policing, you must enable microflow policing of bridged traffic.

For more information, see the "Policers" section on page 43-24.

This example shows how to enable microflow policing of traffic in VLANs 1 through 20:

```
Console> (enable) set qos bridged-microflow-policing enable 1-20
QoS microflow policing is enabled for bridged packets on vlans 1-20.
Console> (enable)
```

Configuring Standard Receive-Queue Tail-Drop Thresholds

To configure the standard receive-queue tail-drop thresholds on the switch, perform this task in privileged mode:

Task	Command
Configure the standard receive-queue tail-drop thresholds.	**set qos drop-threshold** *port_type* **rx queue 1** *thr1 thr2 thr3 thr4*

For more information, see the "Receive Queues" section on page 43-12.

QoS maintains separate configurations for **1q2t**, **1q4t**, and **1p1q4t** ports. This command configures the standard queue. Specify queue 1 (the threshold in the strict-priority queue, when present, is not separately configurable; it uses threshold 4 as specified for queue 1).

The thresholds are all specified as percentages ranging from 1–100. A value of 10 indicates a threshold when the buffer is 10 percent full.

This example shows how to configure the standard receive-queue tail-drop thresholds:

```
Console> (enable) set qos drop-threshold 1q4t rx queue 1 20 40 75 100
Receive drop thresholds for queue 1 set at 20% 40% 75% 100%
Console> (enable)
```

Note You cannot configure a drop threshold in a **1p1q0t** receive queue.

Configuring 2q2t Port Standard Transmit-Queue Tail-Drop Thresholds

To configure the standard transmit-queue tail-drop thresholds on all **2q2t** ports, perform this task in privileged mode:

Task	Command
Configure the standard transmit-queue tail-drop thresholds on all **2q2t** ports.	**set qos drop-threshold** *port_type* **tx queue** *q# thr1 thr2*

Queue number 1 is the low-priority transmit queue and queue number 2 is high priority. In each queue, the low-priority threshold number is 1 and the high-priority threshold number is 2.

The thresholds are all specified as percentages ranging from 1–100. A value of 10 indicates a threshold when the buffer is 10 percent full.

This example shows how to configure the low-priority transmit-queue tail-drop thresholds:

```
Console> (enable) set qos drop-threshold 2q2t tx queue 1 40 100
Transmit drop thresholds for queue 1 set at 40%  100%
Console> (enable)
```

Note You cannot configure the tail-drop thresholds in **1p3q1t** transmit queues.

Configuring Standard Queue WRED-Drop Thresholds

1p2q2t, **1p3q1t**, and **1p2q1t** ports have weighted random early detection (WRED)-drop thresholds in their standard transmit queues.

A **1p1q8t** port has WRED-drop thresholds in its 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 43-29).

RQS Nº 03/ 43-53 N
CPMI - CORREIOS
0709
Fls:
3701
Doc:

To configure the standard queue WRED-drop thresholds on all ports of each type, perform this task in privileged mode:

Task	Command
Configure the standard queue WRED-drop thresholds on all ports of a given type.	**set qos wred 1p2q2t [tx] queue** *q#* [*thr1Lo*:]*thr1Hi* [*thr2Lo*:]*thr2Hi* **set qos wred 1p3q1t [tx] queue** *q#* [*thr1Lo*:]*thr1Hi* **set qos wred 1p1q8t queue** *q#* [*thr1Lo*:]*thr1Hi* [*thr2Lo*:]*thr2Hi* [*thr_n_Lo*:]*thr_n_Hi*... [*thr8Lo*:]*thr8Hi* **set qos wred 1p2q1t [tx] queue** *q#* [*thr1Lo*:]*thr1Hi*

When configuring **1p2q2t** ports, note the following:

- Queue 1 is the low-priority standard transmit queue.
- Queue 2 is the high-priority standard transmit queue.
- When configuring each standard transmit queue, note the following:
  - The first percentage that you enter sets the low-priority threshold.
  - The second percentage that you enter sets the high-priority threshold.

When configuring **1p3q1t** ports, note the following:

- 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.
- When you configure each standard transmit queue, the single percentage that you enter sets the threshold.

When configuring **1p1q8t** ports, note the following:

- Queue 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 1 is the low-priority standard transmit queue.
- Queue 2 is the high-priority standard transmit queue.
- When you configure each standard transmit queue, the single percentage that you enter sets the threshold.

When configuring thresholds, note the following:

- The thresholds are all specified as percentages ranging from 0–100. A value of 10 indicates a threshold when the buffer is 10 percent full.
- You can configure both the low WRED threshold and the high WRED threshold. You must set the low threshold to a lower percentage than the high threshold.
- The low WRED threshold is the traffic level under which no traffic is dropped. The high WRED threshold is the traffic level above which all traffic is dropped. Traffic in the queue between the low and high WRED thresholds has an increasing chance of being dropped as the queue fills. The default low WRED threshold is zero (all traffic has some chance of being dropped).

This example shows how to configure the low-priority transmit-queue WRED-drop thresholds:

```
Console> (enable) set qos wred 1p2q2t queue 1 40:70 70:100
WRED thresholds for queue 1 set to 40:70 and 70:100  on all WRED-capable 1p2q2t ports.
Console> (enable)
```

Note The threshold in the strict-priority queue is not configurable.

Allocating Bandwidth Between Standard Transmit Queues

The switch transmits frames from one standard queue at a time using a weighted-round robin (WRR) algorithm. WRR uses a weight value to decide how much to transmit from one queue before switching to the other. The higher the weight assigned to a queue, the more transmit bandwidth is allocated to it.

To allocate bandwidth between standard transmit queues, perform this task in privileged mode:

Task	Command
Allocate bandwidth between standard transmit queues.	**set qos wrr** *port_type queue1-weight queue2-weight* [*queue3-weight*]

The valid values for the *port_type* parameter are **2q2t**, **1p2q2t**, **1p3q1t**, and **1p2q1t**.

Note **1p2q1t** ports use deficit weighted round robin (DWRR), which transmits from the queues without starving the low-priority queue by keeping track of low-priority queue under-transmission and compensating in the next round.

QoS maintains separate configurations for each port type. This command configures only the standard queues; the strict-priority queue requires no configuration. The valid values for weight range from 1–255.

This example shows how to allocate bandwidth for the **2q2t** ports:

```
Console> (enable) set qos wrr 2q2t 30 70
QoS wrr ratio is set successfully.
Console> (enable)
```


ECT 3408
ROS Nº 03/2005 - CN
CPMI - CORREIOS
43-55
0710
Fls:
Doc: 3701

Configuring the Receive-Queue Size Ratio

For **1p1q0t** and **1p1q8t** ports, estimate the mix of standard-priority and strict-priority traffic on your network (for example, 85 percent standard-priority traffic and 15 percent strict-priority traffic). Specify queue ratios with the estimated percentages, which must range from 1–99 and together add up to 100.

To configure the receive-queue size ratio, perform this task in privileged mode:

Task	Command
Configure the receive-queue size ratio between receive queue 1 (standard priority) and receive queue 2 (strict priority).	**set qos rxq-ratio** {**1p1q0t** | **1p1q8t**} *queue1-val queue2-val*

This example shows how to configure the receive-queue size ratio:

```
Console> (enable) set qos rxq-ratio 1p1q0t 80 20
QoS rxq-ratio is set successfully.
Console> (enable)
```

Configuring the Transmit-Queue Size Ratio

For **2q2t**, **1p2q2t**, and **1p2q1t** ports, estimate the mix of traffic of various priorities on your network (for example, 75 percent low-priority traffic, 15 percent high-priority traffic, and 10 percent strict-priority traffic). Specify queue ratios with the estimated percentages, which must range from 1–99 and together add up to 100.

To configure the transmit-queue size ratio for each port type, perform this task in privileged mode:

Task	Command
Configure the transmit-queue size ratio.	**set qos txq-ratio** {**2q2t** | **1p2q2t** | **1p2q1t**} *queue1-val queue2-val* [*queue3-val*]

This example shows how to configure the transmit-queue size ratio:

```
Console> (enable) set qos txq-ratio 2q2t 80 20
QoS txq-ratio is set successfully.
Console> (enable)
```

Mapping CoS Values to Drop Thresholds

This command associates CoS values with receive- and transmit-queue drop thresholds. QoS maintains separate configurations for each port type.

These sections describe mapping CoS values to drop thresholds:

- Associating 1q4t/2q2t Ports, page 43-57
- Associating 1q2t/1p2q2t and 1p1q4t/1p2q2t Ports, page 43-57
- Associating 1p1q8t/1p2q1t Ports, page 43-59
- Reverting to CoS Map Defaults, page 43-60

Associating 1q4t/2q2t Ports

On **1q4t/2q2t** ports, you configure the receive queues and the transmit queues with the same command.

To associate CoS values to the drop thresholds on **1q4t/2q2t** ports, perform this task in privileged mode:

	Task	Command
Step 1	Associate a CoS value to a drop threshold.	**set qos map 2q2t tx** *q# thr#* **cos** *coslist*
Step 2	Verify the configuration.	**show qos info config** {**1q4t rx** | **2q2t tx** }

The receive- and transmit-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

Use the transmit queue and transmit-queue drop-threshold values in this command. This example shows how to associate the CoS values 0 and 1 to both standard receive-queue 1/threshold 1 and standard transmit-queue 1/threshold 1:

```
Console> (enable) set qos map 2q2t tx 1 1 cos 0,1
Qos tx priority queue and threshold mapped to cos successfully.
Console> (enable)
```

Associating 1q2t/1p2q2t and 1p1q4t/1p2q2t Ports

On **1q2t/1p2q2t** and **1p1q4t/1p2q2t** ports, you configure the receive queues and the transmit queues separately.

1q2t Receive Queues

To associate CoS values to **1q2t** receive-queue drop thresholds, perform this task in privileged mode:

	Task	Command
Step 1	Associate a CoS value to a receive-queue drop threshold.	**set qos map 1q2t rx 1 1 cos** *coslist*
Step 2	Verify the configuration.	**show qos info config 1q2t rx**

Threshold 1 is the low-priority threshold. Threshold 2, the high-priority threshold, is not configurable.

This example shows how to associate the CoS value 3 to high-priority threshold 2:

```
Console> (enable) set qos map 1q2t rx 1 1 cos 3
QoS rx priority queue and threshold mapped to cos successfully.
Console> (enable)
```


RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 0043-57
Doc: 3701

1p1q4t Receive Queues

To associate CoS values to **1p1q4t** receive-queue drop thresholds, perform this task in privileged mode:

	Task	Command
Step 1	Associate a CoS value to a receive-queue drop threshold.	**set qos map 1p1q4t rx** *q# thr#* **cos** *coslist*
Step 2	Verify the configuration.	**show qos info config 1p1q4t rx**

Queue 1 is the standard queue, and queue 2 is the strict-priority queue.

Threshold numbers range from 1 for low priority to 4 for high priority.

This example shows how to associate the CoS value 5 to strict-priority receive-queue 2/threshold 1:

```
Console> (enable) set qos map 1p1q4t rx 2 1 cos 5
Qos rx strict queue and threshold mapped to cos successfully.
Console> (enable)
```

1p2q2t Transmit Queues

To associate CoS values to the **1p2q2t** transmit-queue drop thresholds, perform this task in privileged mode:

	Task	Command
Step 1	Associate a CoS value to a transmit-queue drop threshold.	**set qos map 1p2q2t tx** *q# thr#* **cos** *coslist*
Step 2	Verify the configuration.	**show qos info config 1p2q2t tx**

Queue 1 is standard low priority, queue 2 is high priority, and queue 3 is strict priority.

Threshold 1 is low priority and threshold 2 is high priority.

This example shows how to associate the CoS value 5 to strict-priority transmit-queue 3/drop threshold 1:

```
Console> (enable) set qos map 1p2q2t tx 3 1 cos 5
Qos tx strict queue and threshold mapped to cos successfully.
Console> (enable)
```

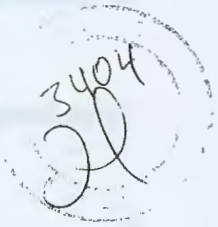
Associating 1p1q0t/1p3q1t Ports

On **1p1q0t/1p3q1t** ports, you configure the receive queues and the transmit queues separately.

1p1q0t Receive Queues

To associate CoS values to **1p1q0t** receive queues, perform this task in privileged mode:

	Task	Command
Step 1	Associate a CoS value to a receive queue.	**set qos map 1p1q0t rx** *q#* **cos** *coslist*
Step 2	Verify the configuration.	**show qos info config 1p1q0t rx**



Queue 1 is the standard queue, and queue 2 is the strict-priority queue.

This example shows how to associate the CoS value 5 to strict-priority receive-queue 2:

```
Console> (enable) set qos map 1p1q0t rx 2 cos 5
QoS queue mapped to cos successfully.
Console> (enable)
```

1p3q1t Transmit Queues

With **1p3q1t** transmit queues, you can associate a CoS value with either the nonconfigurable tail-drop threshold or the configurable WRED-drop threshold as follows:

- To associate a CoS value with the tail-drop threshold, map the CoS value to the queue.
- To associate a CoS value with the WRED-drop threshold, map the CoS value to the queue and threshold.

To associate CoS values to the **1p3q1t** transmit-queue drop thresholds, perform this task in privileged mode:

	Task	Command
Step 1	Associate a CoS value to a transmit-queue drop threshold.	**set qos map 1p3q1t tx** *q#* [*thr#*] **cos** *coslist*
Step 2	Verify the configuration.	**show qos info config 1p3q1t tx**

Queue 1 is the standard low-priority queue, queue 2 is the medium-priority queue, queue 3 is the high-priority queue, and queue 4 is the strict-priority queue.

To map CoS values to the tail-drop threshold, omit the threshold number or enter **0**.

The WRED-drop threshold number is 1.

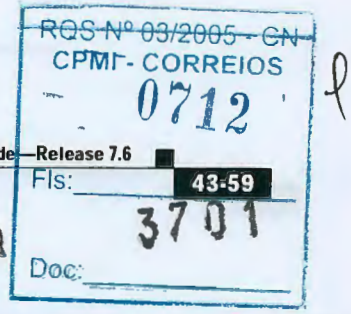
This example shows how to associate the CoS value 0 to transmit-queue 1/drop threshold 1:

```
Console> (enable) set qos map 1p3q1t tx 1 1 cos 0
Qos tx strict queue and threshold mapped to cos successfully.
Console> (enable)
```

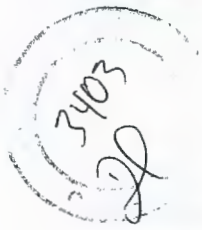
Associating 1p1q8t/1p2q1t Ports

When you configure **1p1q8t/1p2q1t** ports, note the following:

- You configure the receive queues and the transmit queues separately.
- You can associate a CoS value with either the nonconfigurable tail-drop threshold or the configurable WRED-drop threshold:
  - To associate a CoS value with the tail-drop threshold, map the CoS value to the queue.
  - To associate a CoS value with the WRED-drop threshold, map the CoS value to the queue and threshold.



1p1q8t Receive Queues



To associate CoS values to **1p1q8t** receive queues, perform this task in privileged mode:

	Task	Command
Step 1	Associate a CoS value to a receive queue.	**set qos map 1p1q8t rx** *q#* [*thr#*] **cos** *coslist*
Step 2	Verify the configuration.	**show qos info config 1p1q8t rx**

Queue 1 is the standard queue, and queue 2 is the strict-priority queue.

To map CoS values to the tail-drop threshold, omit the threshold number or enter **0**.

The WRED-drop threshold number is 1.

This example shows how to associate the CoS value 5 to strict-priority receive-queue 2:

```
Console> (enable) set qos map 1p1q8t rx 2 cos 5
QoS queue mapped to cos successfully.
Console> (enable)
```

1p2q1t Transmit Queues

To associate CoS values to the **1p2q1t** transmit-queue drop thresholds, perform this task in privileged mode:

	Task	Command
Step 1	Associate a CoS value to a transmit-queue drop threshold.	**set qos map 1p2q1t tx** *q#* [*thr#*] **cos** *coslist*
Step 2	Verify the configuration.	**show qos info config 1p2q1t tx**

Queue 1 is the standard low-priority queue, queue 2 is the standard high-priority queue, and queue 3 is the strict-priority queue.

To map CoS values to the tail-drop threshold, omit the threshold number or enter **0**.

The WRED-drop threshold number is 1.

This example shows how to associate the CoS value 0 to transmit-queue 1/drop threshold 1:

```
Console> (enable) set qos map 1p2q1t tx 1 1 cos 0
Qos tx strict queue and threshold mapped to cos successfully.
Console> (enable)
```

Reverting to CoS Map Defaults

To revert to default CoS value/drop threshold mapping, perform this task in privileged mode:

	Task	Command
Step 1	Revert to CoS map defaults.	**clear qos map** {**1p1q4t rx** | **1p1q0t rx** | **1p2q2t tx** | **2q2t tx** | **1p3q1t tx**}
Step 2	Verify the configuration.	**show qos info config** {**1q4t rx** | **1p1q4t rx** | **1p1q0t rx** | **1p1q8t rx** | **1p2q2t tx** | **2q2t tx** | **1p3q1t tx** | **1p2q1t tx**}

This example shows how to revert to CoS map defaults:

```
Console> (enable) clear qos map lp3q1t tx
Qos map setting cleared.
Console> (enable)
```

Configuring DSCP Value Maps

Note The commands in this section are not supported with a Layer 2 Switching Engine.

These sections describe how DSCP values are mapped to other values:

- Mapping Received CoS Values to Internal DSCP Values, page 43-61
- Mapping Received IP Precedence Values to Internal DSCP Values, page 43-62
- Mapping Internal DSCP Values to Egress CoS Values, page 43-62
- Mapping DSCP Markdown Values, page 43-63

Mapping Received CoS Values to Internal DSCP Values

To map received CoS values to the internal DSCP value (see the "Internal DSCP Values" section on page 43-17), perform this task in privileged mode:

	Task	Command
Step 1	Map received CoS values to internal DSCP values.	**set qos cos-dscp-map** *dscp1 dscp2 dscp3 dscp4 dscp5 dscp6 dscp7 dscp8*
Step 2	Verify the configuration.	**show qos maps** {**config** | **runtime**} [**cos-dscp-map** | **ipprec-dscp-map** | **dscp-cos-map** | **policed-dscp-map**]

Enter 8 DSCP values to which QoS maps received CoS values 0 through 7. This example shows how to map received CoS values to internal DSCP values:

```
Console> (enable) set qos cos-dscp-map 20 30 1 43 63 12 13 8
QoS cos-dscp-map set successfully.
Console> (enable)
```

To revert to default CoS to DSCP value mapping, perform this task in privileged mode:

	Task	Command
Step 1	Revert to CoS value/DSCP value map defaults.	**clear qos cos-dscp-map**
Step 2	Verify the configuration.	**show qos maps** {**config** | **runtime**} [**cos-dscp-map** | **ipprec-dscp-map** | **dscp-cos-map** | **policed-dscp-map**]

This example shows how to revert to CoS-DSCP map defaults:

```
Console> (enable) clear qos cos-dscp-map
QoS cos-dscp-map setting restored to default.
Console> (enable)
```


RQS Nº 03/2005 - CN
CPMI - CORREIOS
0713
Fls:
Doc: 3701

Mapping Received IP Precedence Values to Internal DSCP Values

To map received IP precedence values to the internal DSCP value (see the "Internal DSCP Values" section on page 43-17), perform this task in privileged mode:

	Task	Command
Step 1	Map received IP precedence values to internal DSCP values.	**set qos ipprec-dscp-map** *dscp1 dscp2 dscp3 dscp4 dscp5 dscp6 dscp7 dscp8*
Step 2	Verify the configuration.	**show qos maps** {**config** | **runtime**} [**cos-dscp-map** | **ipprec-dscp-map** | **dscp-cos-map** | **policed-dscp-map**]

Enter 8 internal DSCP values to which QoS maps received IP precedence values 0 through 7. This example shows how to map received IP precedence values to internal DSCP values:

```
Console> (enable) set qos ipprec-dscp-map 20 30 1 43 63 12 13 8
QoS ipprec-dscp-map set successfully.
Console> (enable)
```

To revert to default IP precedence to DSCP value mapping, perform this task in privileged mode:

	Task	Command
Step 1	Revert to IP precedence value to DSCP value map defaults.	**clear qos ipprec-dscp-map**
Step 2	Verify the configuration.	**show qos maps** {**config** | **runtime**} [**cos-dscp-map** | **ipprec-dscp-map** | **dscp-cos-map** | **policed-dscp-map**]

This example shows how to revert to QoS map defaults:

```
Console> (enable) clear qos ipprec-dscp-map
QoS ipprec-dscp-map setting restored to default.
Console> (enable)
```

Mapping Internal DSCP Values to Egress CoS Values

To map internal DSCP values to the egress CoS values that are used for egress port scheduling and congestion avoidance, perform this task in privileged mode:

	Task	Command
Step 1	Map internal DSCP values to egress CoS values.	**set qos dscp-cos-map** *dscp_list:cos ...*
Step 2	Verify the configuration.	**show qos maps** {**config** | **runtime**} [**cos-dscp-map** | **ipprec-dscp-map** | **dscp-cos-map** | **policed-dscp-map**]

For more information, see the "Internal DSCP Values" section on page 43-17 and the "Ethernet Egress Port Scheduling, Congestion Avoidance, and Marking" section on page 43-27.

Enter up to 64 internal DSCP value list/egress CoS value pairs. This example shows how to map internal DSCP values to egress CoS values:

```
Console> (enable) set qos dscp-cos-map 20-25:7 33-38:3
QoS dscp-cos-map set successfully.
Console> (enable)
```

To revert to default DSCP/CoS value mapping, perform this task in privileged mode:

	Task	Command
Step 1	Revert to DSCP value/CoS value map defaults.	**clear qos dscp-cos-map**
Step 2	Verify the configuration.	**show qos maps** {**config** | **runtime**} [**cos-dscp-map** | **ipprec-dscp-map** | **dscp-cos-map** | **policed-dscp-map**]

This example shows how to revert to DSCP-CoS map defaults:

```
Console> (enable) clear qos dscp-cos-map
QoS dscp-cos-map setting restored to default.
Console> (enable)
```

Mapping DSCP Markdown Values

To map DSCP markdown values used by policers, perform this task in privileged mode:

	Task	Command
Step 1	Map DSCP values to markdown DSCP values.	**set qos policed-dscp-map** *dscp_list:markdown_dscp ...*
Step 2	With PFC2, map DSCP values to markdown DSCP values.	**set qos policed-dscp-map** [**normal** | **excess**] *in_profile_dscp_list:policed_dscp ...*
Step 3	Verify the configuration.	**show qos maps** {**config** | **runtime**} [**cos-dscp-map** | **ipprec-dscp-map** | **dscp-cos-map** | **policed-dscp-map**]

For more information, see the "Policers" section on page 43-24.

Enter up to 64 DSCP-value-list/DSCP-value pairs.

This example shows how to map DSCP markdown values:

```
Console> (enable) set qos policed-dscp-map 20-25:7 33-38:3
QoS dscp-dscp-map set successfully.
Console> (enable)
```

This example shows how to map DSCP markdown values for packets exceeding the excess rate:

```
Console> (enable) set qos policed-dscp-map 33:30
QoS normal-rate policed-dscp-map set successfully.
Console> (enable) set qos policed-dscp-map excess-rate 33:30
QoS excess-rate policed-dscp-map set successfully.
Console> (enable)
```

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0714
Fls: 43-63
3701
Doc:

Note Configure marked-down DSCP values that map to CoS values that are consistent with the markdown penalty (see the "Mapping Internal DSCP Values to Egress CoS Values" section on page 43-62).

To revert to default DSCP markdown value mapping, perform this task in privileged mode:

	Task	Command
Step 1	Revert to DSCP markdown map defaults.	**clear qos policed-dscp-map** [**normal-rate** | **excess-rate**]
Step 2	Verify the configuration.	**show qos maps** {**config** | **runtime**} [**cos-dscp-map** | **ipprec-dscp-map** | **dscp-cos-map** | **policed-dscp-map**]

This example shows how to revert to DSCP markdown map defaults:

```
Console> (enable) clear qos policed-dscp-map
QoS dscp-cos-map setting restored to default.
Console> (enable)
```

Note Without the **normal-rate** or the **excess-rate** keywords, the **clear qos policed-dscp-map** command clears only the normal policed-dscp map.

Displaying QoS Information

To display QoS information, perform this task:

Task	Command
Display QoS information.	**show qos info** [**runtime** | **config**]

This example shows how to display the QoS runtime information for port 2/1:

```
Console> show qos info config 2/1
QoS setting in NVRAM:
QoS is enabled
Port 2/1 has 2 transmit queue with 2 drop thresholds (2q2t).
Port 2/1 has 1 receive queue with 4 drop thresholds (1q4t).
Interface type:vlan-based
ACL attached:
The qos trust type is set to untrusted.
Default CoS = 0
Queue and Threshold Mapping:
Queue Threshold CoS
----- --------- ---------------
1     1         0 1
1     2         2 3
2     1         4 5
2     2         6 7
Rx drop thresholds:
Rx drop thresholds are disabled for untrusted ports.
Queue #  Thresholds - percentage (abs values )
-------  ----------------------------------
```

```
1        50% 60% 80% 100%
Tx drop thresholds:
Queue #  Thresholds - percentage (abs values )
-------  ---------------------------------------
1        40% 100%
2        40% 100%
Tx WRED thresholds:
WRED feature is not supported for this port_type.
Queue Sizes:
Queue #  Sizes - percentage (abs values )
-------  ---------------------------------------
1        80%
2        20%
WRR Configuration of ports with speed 1000Mbps:
Queue #  Ratios (abs values )
-------  ---------------------------------------
1        100
2        255
Console> (enable)
```

Displaying QoS Statistics

To display QoS statistics, perform this task:

Task	Command
Display QoS statistics.	**show qos statistics** {*mod*[*/port*] | **l3stats** | **aggregate-policer** [*policer_name*]}

This example shows how to display QoS statistics for port 2/1:

```
Console> (enable) show qos statistics 2/1
On Transmit:Port 2/1 has 2 Queue(s) 2 Threshold(s)
Q #  Threshold #:Packets dropped
---  -----------------------------------------------
1    1:0 pkts, 2:0 pkts
2    1:0 pkts, 2:0 pkts
On Receive:Port 2/1 has 1 Queue(s) 4 Threshold(s)
Q #  Threshold #:Packets dropped
---  -----------------------------------------------
1    1:0 pkts, 2:0 pkts, 3:0 pkts, 4:0 pkts
```

This example shows how to display QoS Layer 3 statistics:

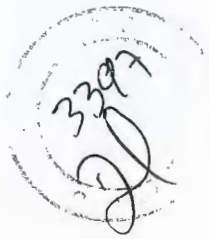
```
Console> (enable) show qos statistics l3stats
QoS Layer 3 Statistics show statistics since last read.
Packets dropped due to policing: 0
IP packets with ToS changed:     0
IP packets with CoS changed:     26
Non-IP packets with CoS changed: 0
Console>
```

This example shows how to display QoS aggregate policer statistics:

```
Console> (enable) show qos statistics aggregate-policer
QoS aggregate-policer statistics:
Aggregate Policer                Packet Count Packets exceed Packets exceed
                                              normal rate    excess rate
-------------------------------- ------------ -------------- -------------
test                                     1000             20
```


RQS Nº 03/2005 - CN
CPMI - CORREIOS
0715
Fls: 43-65
Doc: 3701

Reverting to QoS Defaults



Note Reverting to defaults disables QoS, because QoS is disabled by default.

To revert to QoS defaults, perform this task in privileged mode:

Task	Command
Revert to QoS defaults.	**clear qos config**

This example shows how to revert to QoS defaults:

```
Console> (enable) clear qos config
This command will disable QoS and take values back to factory default.
Do you want to continue (y/n) [n]? y
QoS config cleared.
Console> (enable)
```

Disabling QoS

To disable QoS, perform this task in privileged mode:

Task	Command
Disable QoS on the switch.	**set qos** {**enable** | **disable**}

This example shows how to disable QoS:

```
Console> (enable) set qos disable
QoS is disabled.
Console> (enable)
```

Configuring COPS Support

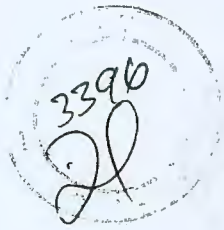
Note The commands in this section are not supported with a Layer 2 Switching Engine.

Note COPS can configure QoS only for IP traffic. Use the CLI or SNMP to configure QoS for all other traffic.

These sections describe configuring COPS support:

- Port ASICs, page 43-67
- Understanding QoS Policy, page 43-67
- Selecting COPS as the QoS Policy Source, page 43-67
- Selecting Locally Configured QoS Policy, page 43-68
- Enabling Use of Locally Configured QoS Policy, page 43-68

- Assigning Port Roles, page 43-69
- Removing Roles from Port ASICs, page 43-69
- Deleting Roles, page 43-70
- Configuring Policy Decision Point Servers, page 43-70
- Deleting the PDP Server Configuration, page 43-70
- Configuring the COPS Domain Name, page 43-71
- Deleting the COPS Domain Name, page 43-71
- Configuring the COPS Communications Parameters, page 43-71



Note Throughout this publication and all Catalyst 6500 series documents, the term *COPS* refers to COPS support as implemented on the Catalyst 6500 series switches.

Port ASICs

Some COPS support features affect all ports that are controlled by a port ASIC. The following sections use the term *per-ASIC* to identify the features that configure all ports on the same port ASIC:

- The port ASICs on Gigabit Ethernet switching modules control up to 4 ports each: 1–4, 5–8, 9–12, and 13–16.
- A port ASIC on 10-Mbps, 10/100-Mbps, and 100-Mbps Ethernet switching modules controls all ports.
- On 10-Mbps, 10/100-Mbps, and 100-Mbps Ethernet switching modules, another set of port ASICs control 12 ports each (1–12, 13–24, 25–36, and 37–48), but COPS cannot configure them.
- Changes to an EtherChannel port apply to all ports in the EtherChannel and to all ports controlled by the ASIC (or ASICs) that control the EtherChannel ports.

Understanding QoS Policy

The term *QoS policy* refers to the QoS values in effect, such as port trust state and which ACLs are applied to ports and VLANs.

Selecting COPS as the QoS Policy Source

QoS uses locally configured QoS values as the default QoS policy source. To select COPS as the QoS policy source, perform this task in privileged mode:

	Task	Command
Step 1	Select COPS as the QoS policy source.	**set qos policy-source {local | cops}**
Step 2	Verify the QoS policy source.	**show qos policy-source**

This example shows how to select COPS as the QoS policy source:

```
Console> (enable) set qos policy-source cops
QoS policy source for the switch set to COPS.
```

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0716
Doc:

```
Console> (enable) show qos policy-source
QoS policy source for the switch set to COPS.
Console> (enable)
```

Selecting COPS as the QoS policy source switches the following values from locally configured values to received COPS values:

- All DSCP maps
- Named and default ACL definitions
- Microflow and aggregate policers
- CoS to queue assignments
- Threshold configuration
- WRR weight and buffer configuration
- Default port CoS and ACL-to-interface attachments

Selecting Locally Configured QoS Policy

To select locally configured QoS policy, perform this task in privileged mode:

	Task	Command
Step 1	Select locally configured QoS policy.	**set qos policy-source {local | cops}**
Step 2	Verify the QoS policy source.	**show qos policy-source**

This example shows how to select locally configured QoS policy:

```
Console> (enable) set qos policy-source local
QoS policy source for the switch set to local.
Console> (enable) show qos policy-source
QoS policy source for the switch set to local.
Console> (enable)
```

Enabling Use of Locally Configured QoS Policy

When enabled, COPS is the default QoS policy source for all ports. You can use locally configured QoS policy on a per-ASIC basis. To enable use of locally configured QoS policy on a port ASIC, perform this task in privileged mode:

	Task	Command
Step 1	Enable use of locally configured QoS policy on a port.	**set port qos policy-source {local | cops}**
Step 2	Verify the QoS policy source for the port.	**show port qos**

This example shows how to enable use of locally configured QoS policy:

```
Console> (enable) set port qos 1/1 policy-source local
QoS policy source set to local on port(s) 1/1-2.
Console> (enable)
```

Assigning Port Roles

COPS does not configure ports using slot number and port number parameters. COPS uses *roles* that you create and assign to port ASICs.

A role is a name that describes the capability of ports (for example, *access* or *mod2_1-4*). QoS supports 64 roles per switch. You can assign more than one role to a port ASIC (for example, *mod2ports1-12* and *access*), with the limitation that the combined length of role names that are assigned to a port ASIC cannot exceed 255 characters.

The role name can be up to 31 characters long, is not case sensitive but may include uppercase and lowercase characters, and may consist of a–z, A–Z, 0–9, the dash character (-), the underscore character (_), and the period character (.). Role names cannot start with the underscore character.

The first assignment of a new role to a port creates the role.

To assign roles to a port ASIC, perform this task in privileged mode:

	Task	Command
Step 1	Assign roles to a port ASIC.	**set port cops** {*mod/port*} **roles** *role1* [*role2*] ...
Step 2	Verify the roles for the port.	**show port cops** [*mod*[*/port*]]

This example shows how to assign two new roles to the ASIC controlling port 2/1:

```
Console> (enable) set port cops 2/1 roles mod2ports1-12 access
New role 'mod2ports1-12' created.
New role 'access' created.
Roles added for port 2/1-12.
Console> (enable)
```

Removing Roles from Port ASICs

To remove a role from a port ASIC, perform this task in privileged mode:

	Task	Command
Step 1	Remove a role from a port ASIC.	**clear port cops** {*mod/port*} {**all-roles** | **roles** *role1* [*role2*] ...}
Step 2	Verify the roles for the port.	**show port cops** [*mod*[*/port*]]

This example shows how to remove a role from a port ASIC:

```
Console> (enable) clear port cops 3/1 roles backbone_port main_port
Roles cleared for port(s) 3/1-4.
Console> (enable)
```


RQS Nº 03/2005 - CN
CPMI - CORREIOS
0717
43-69
Doc:

Deleting Roles

To delete a role (which removes it from all ports), perform this task in privileged mode:

	Task	Command
Step 1	Delete a role.	**clear cops** {**all-roles** | **roles** *role1* [*role2*] ...}
Step 2	Verify the roles for the port.	**show port cops** [*mod*[*/port*]]

This example shows how to delete a role:

```
Console> (enable) clear cops roles backbone_port main_port
Roles cleared.
Console> (enable)
```

Configuring Policy Decision Point Servers

Note COPS and RSVP can use the same policy decision point (PDP) server.

COPS obtains QoS policy from a PDP server. Configure a primary PDP server and optionally, a backup PDP server.

To configure a PDP server, perform this task in privileged mode:

	Task	Command
Step 1	Configure a PDP server.	**set cops server** *ip_address* [*port*] [**primary**] [**diff-serv** | **rsvp**]
Step 2	Verify the PDP server configuration.	**show cops info**

The *ip_address* parameter can be the IP address or the name of the server.

The *port* variable is the PDP server TCP port number.

Use the **diff-serv** keyword to set the address only for COPS.

This example shows how to configure a PDP server:

```
Console> (enable) set cops server my_server1 primary
my_server1 added to the COPS diff-serv server table as primary server.
my_server1 added to the COPS rsvp server table as primary server.
Console> (enable)
```

Deleting the PDP Server Configuration

To delete the PDP server configuration, perform this task in privileged mode:

	Task	Command
Step 1	Delete the PDP server configuration.	**clear cops server** {**all** | *ip_address* [**diff-serv** | **rsvp**]}
Step 2	Verify the PDP server configuration.	**show cops info**

This example shows how to delete the PDP server configuration:

```
Console> (enable) clear cops server all
All COPS diff-serv servers cleared.
All COPS rsvp servers cleared.
Console> (enable)
```

Configuring the COPS Domain Name

PDP servers use a COPS domain name to communicate with policy enforcement point (PEP) devices such as switches. To configure a COPS domain name for the switch, perform this task in privileged mode:

	Task	Command
Step 1	Configure the COPS domain name.	**set cops domain-name** *domain_name*
Step 2	Verify the COPS domain name.	**show cops info**

This example shows how to configure a COPS domain name:

```
Console> (enable) set cops domain-name my_domain
Domain name set to my_domain.
Console> (enable)
```

Deleting the COPS Domain Name

To delete the COPS domain name, perform this task in privileged mode:

	Task	Command
Step 1	Delete the COPS domain name.	**clear cops domain-name**
Step 2	Verify the configuration.	**show cops info**

This example shows how to delete the COPS domain name:

```
Console> (enable) clear cops domain-name
Domain name cleared.
Console> (enable)
```

Configuring the COPS Communications Parameters

To configure the parameters that COPS uses to communicate with the PDP server, perform this task in privileged mode:

	Task	Command
Step 1	Configure the parameters that COPS uses to communicate with the PDP server.	**set cops retry-interval** *initial increment maximum*
Step 2	Verify the configuration.	**show cops info**

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0718
Doc: 3701

Enter the parameters as a number of seconds in the range from 0 to 65535. The value of the *initial* parameter plus the value of the *increment* parameter must not exceed the value of the *maximum* parameter.

This example shows how to configure the parameters that COPS uses to communicate with the PDP server:

```
Console> (enable) set cops retry-interval 15 1 30
Connection retry intervals set.
Console> (enable)
```

Configuring RSVP Support

Note The commands in this section are not supported with a Layer 2 Switching Engine.

These sections describe configuring RSVP null service template and receiver proxy functionality support:

- Enabling RSVP Support, page 43-72
- Disabling RSVP Support, page 43-73
- Enabling Participation in the DSBM Election, page 43-73
- Disabling Participation in the DSBM Election, page 43-73
- Configuring Policy Decision Point Servers, page 43-74
- Deleting the PDP Server Configuration, page 43-74
- Configuring RSVP Policy Timeout, page 43-75
- Configuring RSVP Use of Local Policy, page 43-75

Note Throughout this publication and all Catalyst 6500 series switch documents, the term *RSVP* refers to RSVP null service template and receiver proxy functionality support as implemented on the Catalyst 6500 series switches.

Enabling RSVP Support

To enable RSVP support, perform this task in privileged mode:

	Task	Command
Step 1	Enable RSVP support on the switch.	**set qos rsvp** {**enable** | **disable**}
Step 2	Verify the configuration.	**show qos rsvp info**
Step 3	Display RSVP activity.	**show qos rsvp flow-info**

This example shows how to enable RSVP support:

```
Console> (enable) set qos rsvp enable
RSVP enabled on the switch.
Console> (enable)
```

Disabling RSVP Support

To disable RSVP support, perform this task in privileged mode:

	Task	Command
Step 1	Disable RSVP support on the switch.	**set qos rsvp** {**enable** | **disable**}
Step 2	Verify the configuration.	**show qos rsvp info**

This example shows how to disable RSVP support:

```
Console> (enable) set qos rsvp disable
RSVP disabled on the switch.
Console> (enable)
```

Enabling Participation in the DSBM Election

Catalyst 6500 series switches can serve as the Designated Subnet Bandwidth Manager (DSBM). You can enable participation in the election of the DSBM on a per-port basis.

Note The DSBM is not reelected when additional RSVP devices join the network. To control which device is the DSBM, disable election participation in all devices except the one that you want elected as DSBM. After the DSBM is elected, reenable election participation in other devices, as appropriate for the network configuration.

To enable the participation of a port in the election of the DSBM, perform this task in privileged mode:

	Task	Command
Step 1	Enable the participation of a port in the election of the DSBM.	**set port rsvp** {*mod/port*} **dsbm-election** {**disable** | **enable** *priority*}
Step 2	Verify the configuration of the port.	**show port rsvp** [*mod* | *mod/port*]

The range for the *priority* parameter is from 128 to 255.

This example shows how to enable the participation of ports 2/1 and 3/2 in the election of the DSBM:

```
Console> (enable) set port rsvp 2/1,3/2 dsbm-election enable 232
DSBM enabled and priority set to 232 for ports 2/1,3/2.
Console> (enable)
```

Disabling Participation in the DSBM Election

To disable the participation of a port in the election of the DSBM, perform this task in privileged mode:

	Task	Command
Step 1	Disable the participation of a port in the election of the DSBM.	**set port rsvp** {*mod/port*} **dsbm-election** {**disable** | **enable** *priority*}
Step 2	Verify the configuration.	**show port rsvp show port rsvp** [*mod/port*]

3390
ROS Nº 03/2005 - CN
CPMI - CORREIOS
0719
Fls: 37
43-73
Doc:

This example shows how to disable the participation of port 2/1 in the election of the DSBM:

```
Console> (enable) set port rsvp 2/1 dsbm-election disable
DSBM disabled for port 2/1.
Console> (enable)
```

Configuring Policy Decision Point Servers

Note COPS and RSVP can use the same PDP server.

When the switch is the DSBM, RSVP communicates with a PDP server. Configure a primary PDP server and optionally, a backup PDP server.

To configure a PDP server, perform this task in privileged mode:

	Task	Command
Step 1	Configure a PDP server.	**set cops server** *ip_address* [*port*] [**primary**] [**diff-serv** | **rsvp**]
Step 2	Verify the PDP server configuration.	**show cops info**

The *ip_address* parameter can be the IP address or the name of the server.

The *port* variable is the PDP server TCP port number.

Use the **rsvp** keyword to set the address only for RSVP.

This example shows how to configure a PDP server:

```
Console> (enable) set cops server my_server1 primary rsvp
my_server1 added to the COPS rsvp server table as primary server.
Console> (enable)
```

Deleting the PDP Server Configuration

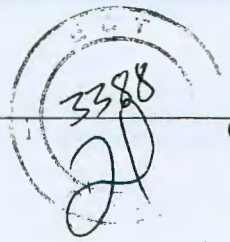
To delete the PDP server configuration, perform this task in privileged mode:

	Task	Command
Step 1	Delete the PDP server configuration.	**clear cops server** {**all** | *ip_address* [**diff-serv** | **rsvp**]}
Step 2	Verify the PDP server configuration.	**show cops info**

Use the **rsvp** keyword to delete only the RSVP address.

This example shows how to delete the PDP server configuration:

```
Console> (enable) clear cops server all
All COPS diff-serv servers cleared.
All COPS rsvp servers cleared.
Console> (enable)
```



Configuring RSVP Policy Timeout

When the switch is the DSBM and communication with the PDP server is lost, the switch continues to function as the DSBM, using cached values, for the period specified by the timeout value; the behavior for new or modified RSVP **path** messages is determined by the RSVP local policy setting.

If communication with the PDP server is not reestablished before the timeout period expires, the switch reverts to the role of the Subnet Bandwidth Manager (SBM) client for all ports and forwards RSVP messages to a newly elected DSBM on the segment. When there is no communication with the PDP server, the switch does not participate in election of the DSBM.

To configure the time that the switch continues to be the DSBM after communication with the PDP server is lost, perform this task in privileged mode:

	Task	Command
Step 1	Configure the RSVP policy timeout.	**set qos rsvp policy-timeout** *timeout*
Step 2	Verify the configuration.	**show qos rsvp info**

Enter the *timeout* parameter as a number of minutes in the range from 0 to 65535 (the default is 30).

This example shows how to configure the RSVP policy timeout:

```
Console> (enable) set qos rsvp policy-timeout 45
RSVP database policy timeout set to 45 minutes.
Console> (enable)
```

Configuring RSVP Use of Local Policy

To configure how RSVP operates after communication with the PDP is lost, perform this task in privileged mode:

	Task	Command
Step 1	Configure how RSVP operates when there is no communication with the PDP server.	**set qos rsvp local-policy** {**forward** | **reject**}
Step 2	Verify the configuration.	**show qos rsvp info**

The **forward** keyword sets the local policy to forward all new or modified RSVP **path** messages. The **reject** keyword sets the local policy to reject all new or modified RSVP **path** messages. This example shows how to change the default local RSVP policy setting to reject all new or modified RSVP **path** messages:

```
Console> (enable) set qos rsvp local-policy reject
RSVP local policy set to reject.
Console> (enable)
```

Note The RSVP local policy is used only until the RSVP policy timeout expires after the connection to the PDP is lost. After the RSVP policy timeout expires, the switch behaves as an SBM client. The RSVP messages pass through the switch unchanged regardless of the RSVP local policy setting. The RSVP local policy setting is not used if the switch never establishes a connection to the PDP.

RQS-Nº 03/2005 - CN
CPMI - CORREIOS
0720
Fls:
43-75
Doc: 3701

Configuring QoS Statistics Data Export

These sections describe how to configure the QoS statistics data export feature:

- Enabling QoS Statistics Data Export Globally, page 43-76
- Enabling Per-Port QoS Statistics Data Export, page 43-77
- Enabling Per-Aggregate Policer QoS Statistics Data Export, page 43-78
- Clearing the Aggregate Policer QoS Statistics, page 43-79
- Setting the QoS Statistics Data Export Time Interval, page 43-79
- Configuring the QoS Statistics Data Export Destination Host and UDP Port, page 43-80
- Displaying QoS Statistics Information, page 43-80

Enabling QoS Statistics Data Export Globally

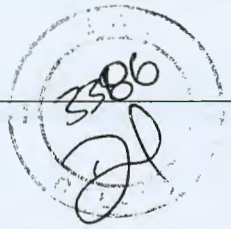
To export QoS statistics data for ports and aggregate policers, you must first configure the feature globally.

To enable QoS statistics data export globally, perform this task in privileged mode:

	Task	Command
Step 1	Enable QoS statistics data export.	**set qos statistics export enable | disable**
Step 2	Verify the configuration.	**show qos statistics export info**

This example shows how to enable QoS statistics data export globally and verify the configuration:

```
Console> (enable) set qos statistics export enable
Export is enabled.
Export destination:172.20.52.3 SYSLOG facility LOG_LOCAL6 (176), severity LOG_DE
BUG (7)
Aggregate policer export is not supported
Console> (enable) show qos statistics export info
Statistics export status and configuration information
-----------------------------------------------------
Export status: enabled
Export time interval: 300
Export destination:172.20.52.3 SYSLOG facility LOG_LOCAL6 (176), severity LOG_DE
BUG (7)
Port    Export
------  --------
 1/1    disabled
 1/2    disabled
 3/1    disabled
 3/2    disabled
 5/1    disabled
 5/2    disabled
 5/3    disabled
 5/4    disabled
<...output truncated...>
Console> (enable)
```



Enabling Per-Port QoS Statistics Data Export

To enable QoS statistics data export on a per-port basis, perform this task in privileged mode:

	Task	Command
Step 1	Enable QoS statistics data export per port.	**set qos statistics export port** *mod/port* **enable | disable**
Step 2	Verify the configuration.	**show qos statistics export info**

Note You must enable QoS statistics data export globally in order for the per-port configuration to take effect.

This example shows how to enable the QoS statistics data export feature per port and verify the configuration:

```
Console> (enable) set qos statistics export port 5/1 enable
Port export enabled on 5/1.
Console> (enable) show qos statistics export info
Statistics export status and configuration information
-----------------------------------------------------
Export status: enabled
Export time interval: 300
Export destination:172.20.52.3 SYSLOG facility LOG_LOCAL6 (176), severity LOG_DE
BUG (7)
Port    Export
------  --------
 1/1    disabled
 1/2    disabled
 3/1    disabled
 3/2    disabled
 5/1    enabled
 5/2    disabled
<output truncated>
Console> (enable)
```

When enabled on a port, 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

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0721
Fls
43-77
Doc: 3701

Enabling Per-Aggregate Policer QoS Statistics Data Export

To enable QoS statistics data export on a per-aggregate policer basis, perform this task in privileged mode:

	Task	Command
Step 1	Enable QoS statistics data export per-aggregate policer.	**set qos statistics export aggregate** *name* {**enable** | **disable**}
Step 2	Verify the configuration.	**show qos statistics export info**

Note You must enable QoS statistics data export globally in order for the per-aggregate policer configuration to take effect.

This example shows how to enable QoS statistics data export for a specific aggregate policer and verify the configuration:

```
Console> (enable) set qos statistics export aggregate ipagg_3 enable
Statistics data export enabled for aggregate policer ipagg_3
Console> (enable) show qos statistics export info
Statistics export status and configuration information
-----------------------------------------------------
Export status: enabled
Export time interval: 300
Export destination:172.20.52.3 SYSLOG facility LOG_LOCAL6 (176), severity LOG_DE
BUG (7)
Port    Export
------  --------
 1/1    disabled
 1/2    disabled
 3/1    disabled
 3/2    disabled
 5/1    enabled
 5/2    disabled
<output truncated>

Aggregate name  Export
--------------  --------
ipagg_3         enabled
Console> (enable)
```

When enabled for a named aggregate policer, QoS statistics data export contains the following fields, separated by the delimiter character:

- Export type ("2" for an aggregate policer)
- Aggregate policer name
- Direction ("in")
- PFC slot number
- Number of in-profile packets
- Number of packets that exceed the CIR
- Number of packets that exceed the PIR
- Time stamp

Clearing the Aggregate Policer QoS Statistics

To clear the aggregate policer QoS statistics, perform this task in privileged mode:

	Task	Command
Step 1	Clear the aggregate policer QoS statistics.	**clear qos statistics aggregate-policer** [*policer_name*]
Step 2	Verify the configuration.	**show qos statistics export info**

This example shows how to clear the QoS aggregate policer statistics for a specific aggregate policer:

```
Console> (enable) clear qos statistics aggregate-policer aggr_1
Aggregate policer 'aggr_1' statistical counters cleared.
```

If you do not specify the aggregate policer, all aggregate policer statistics are cleared:

```
Console> (enable) clear qos statistics aggregate-policer
QoS aggregate policers statistical counters cleared.
```

Setting the QoS Statistics Data Export Time Interval

The default interval at which QoS statistics is exported is 30 seconds. To set the time interval for the QoS statistics data export, perform this task in privileged mode:

	Task	Command
Step 1	Set the time interval for the QoS statistics data export.	**set qos statistics export interval** *interval_seconds*
Step 2	Verify the configuration.	**show qos statistics export info**

This example shows how to set the QoS statistics data export interval and verify the configuration:

```
Console> (enable) set qos statistics export interval 500
Time interval set to 500
Console> (enable) show qos statistics export info
Statistics export status and configuration information
-----------------------------------------------------
Export status: enabled
Export time interval: 500
Export destination:172.20.52.3 SYSLOG facility LOG_LOCAL6 (176), severity LOG_DE
BUG (7)
Port    Export
------  --------
 1/1    disabled
 1/2    disabled
 3/1    disabled
 3/2    disabled
 5/1    enabled
 5/2    disabled
<output truncated>

Aggregate name  Export
--------------  --------
ipagg_3         enabled
Console> (enable)
```


RQS Nº 03/2005 - CN
CPMI - CORREIOS
0722
43-79
Doc: 3701

Configuring the QoS Statistics Data Export Destination Host and UDP Port

To configure the QoS statistics data export destination host and UDP port number, perform this task in privileged mode:

	Task	Command
Step 1	Configure the QoS statistics data export destination host and UDP port number.	**set qos statistics export destination** {*host_name* | *ip_address*} [**syslog** [*facility* | *severity*] *port*]
Step 2	Verify the configuration.	**show qos statistics export info**

This example shows how to configure the QoS statistics data export destination host and UDP port number and verify the configuration:

```
Console> (enable) set qos statistics export destination stargate 9996
Statistics data export destination set to stargate port 9996.
Console> (enable) show qos statistics export info
Statistics export status and configuration information
-----------------------------------------------------
Export status: enabled
Export time interval: 500
Export destination:Stargate, UDP port 9996
Port    Export
------  --------
 1/1    disabled
 1/2    disabled
 3/1    disabled
 3/2    disabled
 5/1    enabled
 5/2    disabled
<output truncated>

Aggregate name  Export
--------------  --------
ipagg_3         enabled
Console> (enable)
```

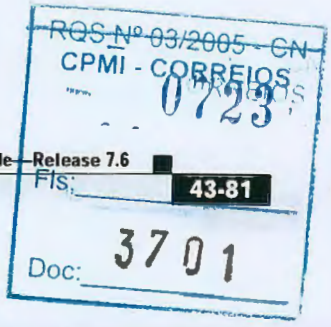
Displaying QoS Statistics Information

To display the QoS statistics per-port and per-aggregate policer packet and byte rates, perform this task in privileged mode:

Task	Command
Display the QoS statistics per-port and per-aggregate policer packet and byte rates.	**show mac** [**utilization**] [*mod*[/*port*]]

This example shows how to display the QoS statistics per-port and per-aggregate policer packet and byte rates:

```
Console> (enable) show mac utilization 1

5 min input/output port rates:

Port  Xmit-Packet-Rate     Xmit-Octet-Rate
----- -------------------- --------------------
1/1                  1343               123432
1/2                  2342               232343
Port  Rcv-Packet-Rate      Rcv-Octet-Rate
----- -------------------- --------------------
1/1                  1324               143253
1/2                  2234               253234
Console>(enable)
```



Ap BO

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0724
Fls:
Doc: 3701

CHAPTER 38

Configuring SPAN and RSPAN

This chapter describes how to configure Switched Port Analyzer (SPAN) and Remote SPAN (RSPAN) 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 Command Reference* publication.

This chapter consists of these sections:

- Understanding How SPAN and RSPAN Works, page 38-1
- SPAN and RSPAN Session Limits, page 38-4
- Configuring SPAN, page 38-5
- Configuring RSPAN, page 38-9

Note To configure SPAN or RSPAN from a network management station (NMS), refer to the NMS documentation (see the "Using CiscoWorks2000" section on page 36-6).

Understanding How SPAN and RSPAN Works

These sections describe the concepts and terminology associated with SPAN and RSPAN configuration:

- SPAN Session, page 38-2
- Destination Port, page 38-2
- Source Port, page 38-2
- Ingress SPAN, page 38-3
- Egress SPAN, page 38-3
- VSPAN, page 38-3
- Trunk VLAN Filtering, page 38-4
- SPAN Traffic, page 38-4

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0725
Fls:
Doc:

SPAN Session

A SPAN session is an association of a destination port with a set of source ports, configured with parameters that specify the monitored network traffic. You can configure multiple SPAN sessions in a switched network. SPAN sessions do not interfere with the normal operation of the switches. You can enable or disable SPAN sessions with command-line interface (CLI) or SNMP commands. When enabled, a SPAN session might become active or inactive based on various events or actions, and this would be indicated by a syslog message. The "Status" field in the **show span** and **show rspan** commands displays the operational status of a SPAN or RSPAN session.

A SPAN or RSPAN destination session remains inactive after system power up until the destination port is operational. An RSPAN source session remains inactive until any of the source ports are operational or the RSPAN VLAN becomes active.

Destination Port

A destination port (also called a *monitor port*) is a switch port where SPAN sends packets for analysis. After a port becomes an active destination port, it does not forward any traffic except that required for the SPAN session. By default, an active destination port disables incoming traffic (from the network to the switching bus), unless you specifically enable the port. If incoming traffic is enabled for the destination port, it is switched in the native VLAN of the destination port. The destination port does not participate in spanning tree while the SPAN session is active. See the caution statement in the "Configuring SPAN from the CLI" section on page 38-6 for information on how to prevent loops in your network topology.

Only one destination port is allowed per SPAN session, and the same port cannot be a destination port for multiple SPAN sessions. A switch port configured as a destination port cannot be configured as a source port. EtherChannel ports cannot be SPAN destination ports.

If the trunking mode of a SPAN destination port is "on" or "nonegotiate" during SPAN session configuration, the SPAN packets forwarded by the destination port have the encapsulation as specified by the trunk type; however, the destination port stops trunking, and the **show trunk** command reflects the trunking status for the port prior to SPAN session configuration.

Source Port

A source port is a switch port monitored for network traffic analysis. The traffic through the source ports can be categorized as ingress, egress, or both. You can monitor one or more source ports in a single SPAN session with user-specified traffic types (ingress, egress, or both) applicable for all the source ports.

You can configure source ports in any VLAN. You can configure VLANs as source ports (*src_vlans*), which means that all ports in the specified VLANs are source ports for the SPAN session.

Source ports are administrative (*Admin Source*) or operational (*Oper Source*) or both. Administrative source ports are the source ports or source VLANs specified during SPAN session configuration. Operational source ports are the source ports monitored by the destination port. For example, when source VLANs are used as the administrative source, the operational source is all the ports in all the specified VLANs.

The operational sources are always active ports. If a port is not in the spanning tree, it is not an operational source. All physical ports in an EtherChannel source are included in operational sources if the logical port is included in the spanning tree.

The destination port, if it belongs to any of the administrative source VLANs, is excluded from the operational source.

You can configure a port as a source port in multiple active SPAN sessions, but you cannot configure an active source port as a destination port for any SPAN session.

If a SPAN session is inactive, the "oper source" field is not updated until the session becomes active.

Trunk ports can be configured as source ports and can be mixed with nontrunk source ports; however, the encapsulation of the packets forwarded by the destination port are determined by the trunk settings of the destination port during SPAN session configuration.

Ingress SPAN

Ingress SPAN copies network traffic received by the source ports for analysis at the destination port.

Egress SPAN

Egress SPAN copies network traffic transmitted from the source ports for analysis at the destination port.

VSPAN

VLAN-based SPAN (VSPAN) is analysis of the network traffic in one or more VLANs. You can configure VSPAN as ingress SPAN, egress SPAN, or both. All the ports in the source VLANs become operational source ports for the VSPAN session. The destination port, if it belongs to any of the administrative source VLANs, is excluded from the operational source. If you add or remove ports from the administrative source VLANs, the operational sources are modified accordingly.

Use the following guidelines for VSPAN sessions:

- Trunk ports are included as source ports for VSPAN sessions, but only the VLANs that are in the Admin source list are monitored, provided these VLANs are active for the trunk.
- For VSPAN sessions with both ingress and egress SPAN configured, the system operates as follows based upon the type of supervisor engine you have:
  - WS-X6K-SUP1A-PFC, WS-X6K-SUP1A-MSFC—Two packets are forwarded by the SPAN destination port if the packets get switched on the same VLAN.
  - WS-X6K-SUP1-2GE, WS-X6K-SUP1A-2GE—Only one packet is forwarded by the SPAN destination port.
- An inband port is not included as Oper source for VSPAN sessions.
- When a VLAN is cleared, it is removed from the source list for VSPAN sessions.
- A VSPAN session is disabled if the Admin source VLANs list is empty.
- Inactive VLANs are not allowed for VSPAN configuration.
- A VSPAN session is made inactive if any of the source VLANs become RSPAN VLANs.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0726
Fls:
Doc: 3701

Trunk VLAN Filtering

Trunk VLAN filtering is analysis of network traffic on a selected set of VLANs on trunk source ports. You can combine trunk VLAN filtering with other source ports that belong to any of the selected VLANs, and you can also use trunk VLAN filtering for RSPAN. Based on the traffic type (ingress, egress, or both), SPAN sends a copy of the network traffic in the selected VLANs to the destination port.

Use trunk VLAN filtering only with trunk source ports. If you combine trunk VLAN filtering with other source ports that belong to VLANs not included in the selected list of filter VLANs, SPAN includes only the ports that belong to one or more of the selected VLANs in the operational sources.

When a VLAN is cleared, it is removed from the VLAN filter list. A SPAN session is disabled if the VLAN filter list becomes empty.

Trunk VLAN filtering is not applicable to VSPAN sessions.

SPAN Traffic

All network traffic, including multicast and bridge protocol data unit (BPDU) packets, can be monitored using SPAN (RSPAN does not support monitoring of BPDU packets). Multicast packet monitoring is enabled by default.

In some SPAN configurations, multiple copies of the same source packet are sent to the SPAN destination port. For example, a bidirectional (both ingress and egress) SPAN session is configured for sources a1 and a2 to a destination port d1. If a packet enters the switch through a1 and gets switched to a2, both incoming and outgoing packets are sent to destination port d1. Both packets would be the same (if a Layer-3 rewrite occurs, the packets are different). For RSPAN sessions with sources distributed in multiple switches, the destination ports might forward multiple copies of the same packet.

SPAN and RSPAN Session Limits

You can configure (and store in NVRAM) a maximum of 30 SPAN sessions in a Catalyst 6500 series switch. See Table 38-1 for the supported combinations of SPAN/RSPAN sessions. You can configure multiple ports or VLANs as sources for each session.

Table 38-1 SPAN and RSPAN Session Limits

SPAN/RSPAN Sessions	Catalyst 6500 Series Switches[1]
rx or **both** SPAN sessions	2
tx SPAN sessions	4
tx, **rx**, or **both** RSPAN source sessions	1
RSPAN destinations	24
Total SPAN sessions	30[2]

1. When an RSPAN source session is configured, it will reduce the limit for **rx** or **both** SPAN sessions by one.
2. 2 **rx** or **both** SPAN sessions + 4 **tx** SPAN sessions + 24 RSPAN destination sessions = 30 total SPAN sessions.

Configuring SPAN

These sections describe how to configure SPAN:

- SPAN Hardware Requirements, page 38-5
- Understanding How SPAN Works, page 38-5
- SPAN Configuration Guidelines, page 38-6
- Configuring SPAN from the CLI, page 38-6

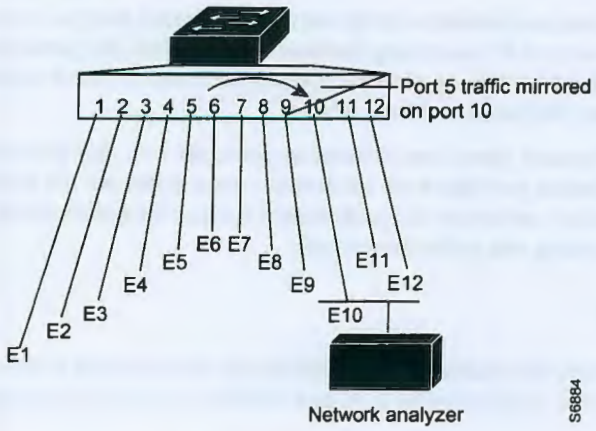
SPAN Hardware Requirements

All Catalyst 6500 series switch supervisor engines support the SPAN feature.

Understanding How SPAN Works

SPAN selects network traffic for analysis by a network analyzer such as a SwitchProbe device or other Remote Monitoring (RMON) probe. SPAN mirrors traffic from one or more source ports on any VLAN, from one or more VLANs, or from the sc0 console interface to a destination port for analysis (see Figure 38-1). In Figure 38-1, all traffic on Ethernet port 5 (the source port) is mirrored to Ethernet port 10. A network analyzer on Ethernet port 10 receives all network traffic from Ethernet port 5 without being physically attached to it.

Figure 38-1 SPAN Configuration



For SPAN configuration, the source ports and the destination port must be on the same switch.

SPAN does not affect the switching of network traffic on source ports; a copy of the packets received or transmitted by the source ports are sent to the destination port.

ROS Nº 03/2005 - CN
CPMI - CORREIOS
0727
Fls:
3701
Doc:

SPAN Configuration Guidelines

Follow these guidelines when configuring SPAN:

- Use a network analyzer to monitor ports.
- For SPAN source ports, SPAN is not supported with ATM ports; it works with Ethernet 10/100/1000-Mbps ports and 10-Gbps ports.
- When enabled, SPAN uses any previously entered configuration. If you have not entered any configuration commands, SPAN uses default parameters.
- If you specify multiple SPAN source ports, the ports can belong to different VLANs.
- See the "SPAN and RSPAN Session Limits" section on page 38-4.
- RSPAN sessions can coexist with SPAN sessions within the SPAN/RSPAN limits described in the "SPAN and RSPAN Session Limits" section on page 38-4.
- The **inpkts** option is disabled by default. Use the **inpkts** keyword with the **enable** option to allow the SPAN destination port to receive normal incoming traffic. Use the **disable** option to prevent the SPAN destination port from receiving normal incoming traffic.
- When you enable the **inpkts** option, a warning message notifies you that the destination port does not support the Spanning Tree Protocol (STP) and may cause loops if you enable this option.
- Learning is enabled by default. Use the **inpkts** keyword with the **learning** option to enable or disable learning for a specific port.
- You can specify a Multilayer Switch Module (MSM) port as the SPAN source port. However, you cannot specify an MSM port as the SPAN destination port.
- When you configure multiple SPAN sessions, the destination module number/port number must be known to index the particular SPAN session.
- If you do not specify the keyword **create** with the **set span** command and you have only one session, the session will be overwritten. If a matching destination port exists, the particular session will be overwritten (with or without specifying **create**). If you specify the keyword **create** and there is no matching destination port, the session will be created.
- If any VLANs on SPAN source port(s) are blocked by spanning tree, you may see extra packets transmitted on the destination port that were not actually transmitted out the source port(s). The extra packets seen at the destination port are packets sent through the switch fabric to the source port and then blocked by spanning tree at the source port.

Configuring SPAN from the CLI

To configure SPAN, you specify the source, the destination port, the direction of the traffic through the source that you want to mirror to the destination port, and whether or not the destination port can receive packets.

To configure a SPAN port, perform this task in privileged mode:

	Task	Command
Step 1	Configure the SPAN source and destination ports.	**set span** {*src_mod/src_ports* | *src_vlans* | **sc0**} {*dest_mod/dest_port*} [**rx** | **tx** | **both**] [**inpkts** {**enable** | **disable**}] [**learning** {**enable** | **disable**}] [**multicast** {**enable** | **disable**}] [**filter** *vlans...*] [**create**]
Step 2	Verify the SPAN configuration.	**show span**

Caution If the SPAN destination port is connected to another device and you enable reception of incoming packets (using the **inpkts enable** keywords), the SPAN destination port receives traffic for whatever VLAN to which the SPAN destination port belongs. The SPAN destination port does *not* participate in spanning tree for that VLAN. Use caution when using the **inpkts** keyword to avoid creating network loops with the SPAN destination port or assigning the SPAN destination port to an unused VLAN.

This example shows how to configure SPAN so that both transmit and receive traffic from port 1/1 (the SPAN source) is mirrored on port 2/1 (the SPAN destination):

```
Console> (enable) set span 1/1 2/1

Destination      : Port 2/1
Admin Source     : Port 1/1
Oper Source      : Port 1/1
Direction        : transmit/receive
Incoming Packets: disabled
Learning         : enabled
Multicast        : enabled
Filter           : -
```

This example shows how to set VLAN 522 as the SPAN source and port 2/1 as the SPAN destination:

```
Console> (enable) set span 522 2/1

Destination      : Port 2/1
Admin Source     : VLAN 522
Oper Source      : Port 3/1-2
Direction        : transmit/receive
Incoming Packets: disabled
Learning         : enabled
Multicast        : enabled
Filter           : -
Console> (enable)
```

This example shows how to set VLAN 522 as the SPAN source and port 2/12 as the SPAN destination. Only transmit traffic is monitored. Normal incoming packets on the SPAN destination port are allowed.

```
Console> (enable) set span 522 2/12 tx inpkts enable

Destination      : Port 2/12
Admin Source     : VLAN 522
Oper Source      : Port 2/1-2
Direction        : transmit
Incoming Packets: enabled
Learning         : enabled
Multicast        : enabled
Filter           : -
Console> (enable)
```

3374
RQS Nº 03/2005 - CN
CPMI - CORREIOS
0728
Fls:
Doc 5701

This example shows how to set port 3/2 as the SPAN source and port 2/2 as the SPAN destination:

```
Console> (enable) set span 3/2 2/2 tx create

Destination      : Port 2/1
Admin Source     : port 3/1
Oper Source      : Port 3/1
Direction        : transmit/receive
Incoming Packets: disabled
```

```
Destination      : Port 2/2
Admin Source     : port 3/2
Oper Source      : Port 3/2
Direction        : transmit
Incoming Packets: disabled
Learning         : enabled
Multicast        : enabled
Filter           : -
Console> (enable)
```

To disable SPAN, perform this task in privileged mode:

Task	Command
Disable SPAN on the switch.	**set span disable** [*dest_mod/dest_port* | *all*]

This example shows how to disable SPAN on the switch:

```
Console> (enable) set span disable 2/1
This command will disable your span session.
Do you want to continue (y/n) [n]?y
Disabled port 2/1 to monitor transmit traffic of VLAN 522
Console> (enable)
```

Configuring RSPAN

These sections describe how to configure RSPAN:

- RSPAN Hardware Requirements, page 38-9
- Understanding How RSPAN Works, page 38-10
- RSPAN Configuration Guidelines, page 38-10
- Configuring RSPAN, page 38-11
- RSPAN Configuration Examples, page 38-14

RSPAN Hardware Requirements

RSPAN supervisor engine requirements are as follows:

- For source switches—Catalyst 6500 series switch with any of the following:
  - Supervisor Engine 1 and Policy Feature Card (PFC): WS-X6K-SUP1A-PFC
  - Supervisor Engine 1, PFC, and Multilayer Switch Feature Card (MSFC): WS-X6K-SUP1A-MSFC
  - Supervisor Engine 1, PFC, and MSFC2: WS-X6K-S1A-MSFC2
  - Supervisor Engine 2 and PFC2: WS-X6K-S2-PFC2
  - Supervisor Engine 2, PFC2, and MSFC2: WS-X6K-S1A-MSFC2
- For destination or intermediate switches—Any Cisco switch supporting RSPAN VLAN

No third party or other Cisco switches can be placed in the end-to-end path for RSPAN traffic.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 0729
Doc: 3701

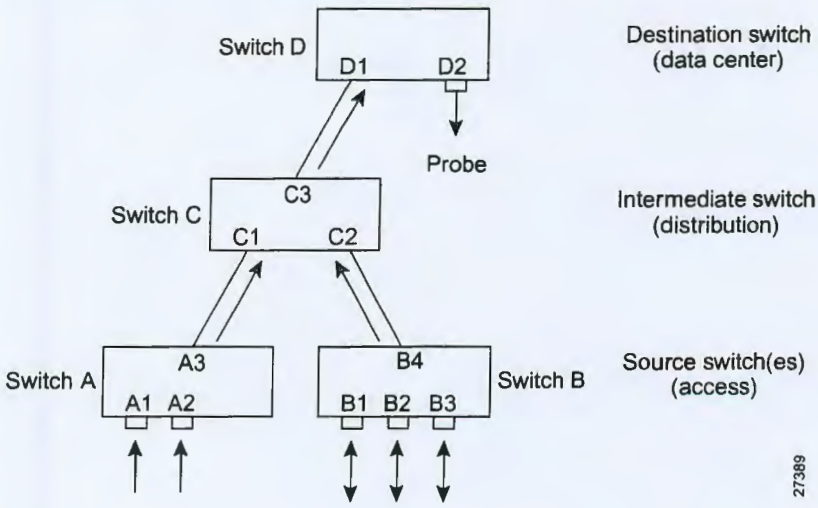
Understanding How RSPAN Works

Note See the "Understanding How SPAN and RSPAN Works" section on page 38-1 for concepts and terminology that apply to both SPAN and RSPAN configuration.

RSPAN has all the features of SPAN (see the "Understanding How SPAN Works" section on page 38-5), plus support for source ports and destination ports distributed across multiple switches, allowing remote monitoring of multiple switches across your network (see Figure 38-2).

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 SPAN traffic from the sources, which cannot be in the RSPAN VLAN, is switched to the RSPAN VLAN and then forwarded to destination ports configured in the RSPAN VLAN. The traffic type for sources (ingress, egress, or both) in an RSPAN session can be different in different source switches but is the same for all sources in each source switch for each RSPAN session. Do not configure any ports in an RSPAN VLAN except those selected to carry RSPAN traffic. Learning is disabled on the RSPAN VLAN.

Figure 38-2 RSPAN Configuration



RSPAN Configuration Guidelines

Follow these guidelines when configuring RSPAN:

Tip As RSPAN VLANs have special properties, we recommend that you reserve a few VLANs across your network for use as RSPAN VLANs. Do not assign access ports to these VLANs.

Tip You can apply an output access control list (ACL) to RSPAN traffic to selectively filter specific flows. Specify these ACLs on the RSPAN VLAN in the RSPAN source switches.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0730
Fls: 3701
Doc: 78-14924-01

- All the items in the "SPAN Configuration Guidelines" section on page 38-6 apply to RSPAN.
- RSPAN sessions can coexist with SPAN sessions within the SPAN/RSPAN limits described in the "SPAN and RSPAN Session Limits" section on page 38-4.
- For RSPAN configuration, you can distribute the source ports and the destination port across multiple switches.
- For RSPAN, trunking is required if you have a source switch with all source ports in one VLAN (VLAN 2 for example) and it is connected to the destination switch through an uplink port that is also in VLAN 2. With RSPAN, the traffic is forwarded to remote switches in the RSPAN VLAN. The RSPAN VLAN is configured only on trunk ports and not on access ports.
- The learning option applies to RSPAN destination ports only.
- RSPAN does not support BPDU packet monitoring.
- To optimize bandwidth utilization in the connecting links, you can configure quality of service (QoS) parameters for the RSPAN VLAN in each of the participating source, intermediate, or destination switches.
- Each Catalyst 6500 series switch can source a maximum of one RSPAN session (ingress, egress, or both). When you configure a remote ingress or bidirectional SPAN session in a source switch, the limit for local ingress or bidirectional SPAN sessions is reduced to one. There are no limits on the number of RSPAN sessions carried across the network within the RSPAN session limits (see the "SPAN and RSPAN Session Limits" section on page 38-4).
- RSPAN VLANs cannot be included as sources for port-based RSPAN sessions when source trunk ports have active RSPAN VLANs. Additionally, RSPAN VLANs cannot be sources in VSPAN sessions.
- You can configure any VLAN as an RSPAN VLAN as long as these conditions are met:
  - The same RSPAN VLAN is used for an RSPAN session in all the switches.
  - All participating switches have appropriate hardware and software.
  - No access port (including the sc0 interface) is configured in the RSPAN VLAN.
- If you enable VLAN Trunking Protocol (VTP) and VTP pruning, RSPAN traffic is pruned in the trunks to prevent the unwanted flooding of RSPAN traffic across the network.
- If you enable GARP VLAN Registration Protocol (GVRP) and GVRP requests conflict with existing RSPAN VLANs, you might observe unwanted traffic in the respective RSPAN sessions.
- You can use RSPAN VLANs in Inter-Switch Link (ISL) to dot1q mapping. However, ensure that the special properties of RSPAN VLANs are supported in all the switches to avoid unwanted traffic in these VLANs.

Configuring RSPAN

The first step in configuring an RSPAN session is to select an RSPAN VLAN for the RSPAN session that *does not* exist in any of the switches that will participate in RSPAN. With VTP enabled in the network, you can create the RSPAN VLAN in one switch and VTP propagates it to the other switches in the VTP domain.

Use VTP pruning to get efficient flow of RSPAN traffic, or manually delete the RSPAN VLAN from all trunks that do not need to carry the RSPAN traffic.

Once the RSPAN VLAN is created, you configure the source and destination switches using the **set rspan** command.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0731
Fls:
3701

To configure RSPAN VLANs, perform this task in privileged mode:

	Task	Command
Step 1	Configure RSPAN VLANs.	**set vlan** *vlan* **[rspan]**
Step 2	Verify the RSPAN VLAN configuration.	**show vlan**

This example shows how to set VLAN 500 as an RSPAN VLAN:

```
Console> (enable) set vlan 500 rspan
vlan 500 configuration successful
Console> (enable)
Console> (enable) show vlan
.
display truncated
.
VLAN DynCreated  RSPAN
---- ---------- --------
1    static     disabled
2    static     disabled
3    static     disabled
99   static     disabled
500  static     enabled
Console> (enable)
```

To configure RSPAN source ports, perform this task in privileged mode:

	Task	Command
Step 1	Configure RSPAN source ports. Use this command on each of the source switches participating in RSPAN.	**set rspan source** {*mod/ports...* | *vlans...* | **sc0**} {*rspan_vlan*} **[rx | tx | both] [multicast {enable | disable}] [filter** *vlans...***] [create]**
Step 2	Verify the RSPAN configuration.	**show rspan**

This example shows how to specify ports 4/1 and 4/2 as ingress source ports for RSPAN VLAN 500:

```
Console> (enable) set rspan source 4/1-2 500 rx
Rspan Type      : Source
Destination     : -
Rspan Vlan      : 500
Admin Source    : Port 4/1-2
Oper Source     : None
Direction       : receive
Incoming Packets: -
Learning        : -
Multicast       : enabled
Filter          : -
Console> (enable)
```

To configure RSPAN source VLANs, perform this task in privileged mode:

	Task	Command
Step 1	Configure RSPAN source VLANs. All the ports in the source VLAN become operational source ports.	**set rspan source** {*mod/ports...* | *vlans...* | **sc0**} {*rspan_vlan*} [**rx** | **tx** | **both**] [**multicast** {**enable** | **disable**}] [**filter** *vlans...*] [**create**]
Step 2	Verify the RSPAN configuration.	**show rspan**

This example shows how to specify VLAN 200 as a source VLAN for RSPAN VLAN 500 (selecting the **rx** option makes all the ports in the VLAN ingress ports):

```
Console> (enable) set rspan source 200 500 rx
Rspan Type      : Source
Destination     : -
Rspan Vlan      : 500
Admin Source    : VLAN 200
Oper Source     : None
Direction       : receive
Incoming Packets: -
Learning        : -
Multicast       : enabled
Filter          : -
Console> (enable)
```

To configure RSPAN destination ports, perform this task in privileged mode:

	Task	Command
Step 1	Configure RSPAN destination ports. Use this command on each of the destination switches participating in RSPAN.	**set rspan destination** {*mod/port*} {*rspan_vlan*} [**inpkts** {**enable** | **disable**}] [**learning** {**enable** | **disable**}] [**create**]
Step 2	Verify the RSPAN configuration.	**show rspan**

```
Console> (enable) set rspan destination 3/1 500
Rspan Type      : Destination
Destination     : Port 3/1
Rspan Vlan      : 500
Admin Source    : -
Oper Source     : -
Direction       : -
Incoming Packets: disabled
Learning        : enabled
Multicast       : -
Filter          : -
Console> (enable)
```

To disable RSPAN, perform this task in privileged mode:

Task	Command
Disable RSPAN on the switch.	**set rspan disable source** [*rspan_vlan* | **all**] **set rpsan disable destination** [*mod/port* | **all**]

ROS Nº 03/2005 - CN
CPMI - CORREIOS
0732
Fls:
3701
Doc:

This example shows how to disable all enabled source sessions:

```
Console> (enable) set rspan disable source all
This command will disable all remote span source session(s).
Do you want to continue (y/n) [n]? y
Disabled monitoring of all source(s) on the switch for remote span.
Console> (enable)
```

This example shows how to disable one source session by *rspan_vlan* number:

```
Console> (enable) set rspan disable source 903
Disabled monitoring of all source(s) on the switch for rspan_vlan 903.
Console> (enable)
```

This example shows how to disable all enabled destination sessions:

```
Console> (enable) set rspan disable destination all
This command will disable all remote span destination session(s).
Do you want to continue (y/n) [n]? y
Disabled monitoring of remote span traffic for all rspan destination ports.
Console> (enable)
```

This example shows how to disable one destination session by *mod/port*:

```
Console> (enable) set rspan disable destination 4/1
Disabled monitoring of remote span traffic on port 4/1.
Console> (enable)
```

RSPAN Configuration Examples

These sections describe how to configure RSPAN:

- Configuring a Single RSPAN Session, page 38-14
- Modifying an Active RSPAN Session, page 38-15
- Adding RSPAN Source Ports in Intermediate Switches, page 38-16
- Configuring Multiple RSPAN Sessions, page 38-16
- Adding Multiple Network Analyzers to an RSPAN Session, page 38-18

Configuring a Single RSPAN Session

This example shows how to configure a single RSPAN session. Figure 38-3 shows an RSPAN configuration; see Table 38-2 for the necessary commands to configure this RSPAN session. Table 38-2 assumes that you have already set up RSPAN VLAN 901 for this session on all the switches using the **set vlan** *vlan* **rspan** command. With VTP enabled in the network, you can create the RSPAN VLAN in one switch and VTP propagates it to the other switches in the VTP domain. Note that in the configuration example shown in Table 38-2, the RSPAN session may be disabled in Switch A or B or both without modifying the configuration in Switch C or Switch D.

Figure 38-3 Single RSPAN Session

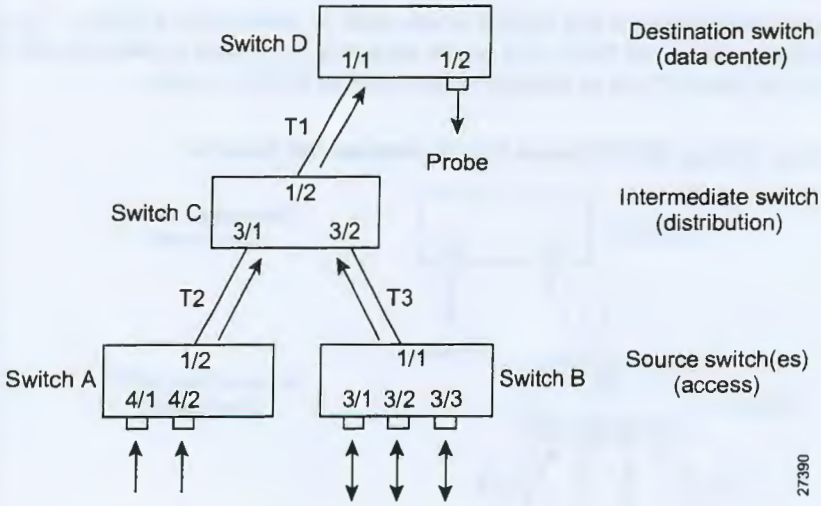


Table 38-2 Configuring a Single RSPAN Session

Switch	Ports	RSPAN VLAN	Direction	RSPAN CLI Commands
A (source)	4/1, 4/2	901	Ingress	**set rspan source 4/1-2 901 rx**
B (source)	3/1, 3/2, 3/3	901	Bidirectional	**set rspan source 3/1-3 901**
C (intermediate)	–	901	–	No RSPAN CLI command needed
D (destination)	1/2	901	–	**set rspan destination 1/2 901**

Modifying an Active RSPAN Session

This example shows how to modify an active RSPAN session. Use Figure 38-3 for reference; see Table 38-3 for the necessary commands to disable an RSPAN session and to add or remove source ports from an RSPAN session.

Table 38-3 Making Modifications to an Active RSPAN Session

Switch	Action	RSPAN CLI Commands
A (source)	Disable the RSPAN session.	**set rspan disable source 901**
B (source)	Remove source port 3/2 from RSPAN session.	**set rspan source 3/1, 3/3 901**
B (source)	Add back source port 3/2 to RSPAN session.	**set rspan source 3/1-3 901**

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 0733
Doc: 3701

Adding RSPAN Source Ports in Intermediate Switches

This example shows how to add RSPAN source ports in intermediate switches. Figure 38-4 shows an RSPAN configuration; see Table 38-4 for the necessary commands to configure this RSPAN session. Ports 2/1-2 in Switch C can be configured for the same RSPAN session.

Figure 38-4 Adding RSPAN Source Ports in Intermediate Switches

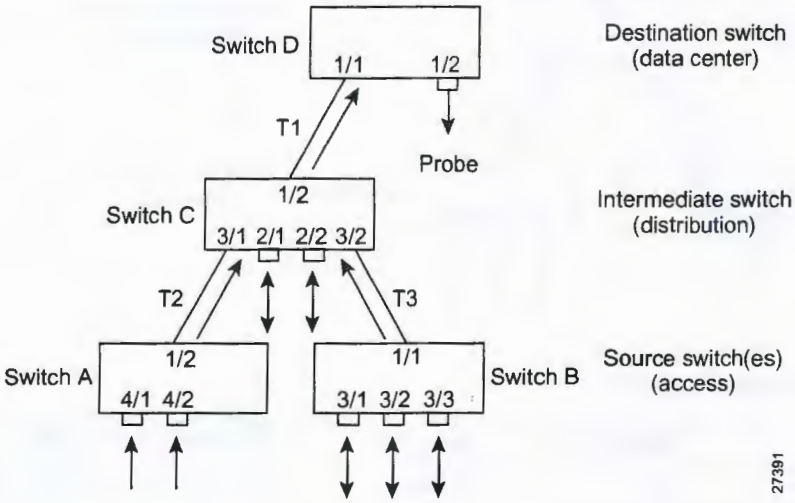


Table 38-4 Adding RSPAN Source Ports in Intermediate Switches

Switch	Ports	RSPAN VLAN	Direction	RSPAN CLI Commands
A (source)	4/1, 4/2	901	Ingress	**set rspan source 4/1-2 901 rx**
B (source)	3/1, 3/2, 3/3	901	Bidirectional	**set rspan source 3/1-3 901**
C (intermediate)	–	901	–	No RSPAN CLI command needed
C (source)	2/1, 2/2	901	Bidirectional	**set rspan source 2/1-2 901**
D (destination)	1/2	901	–	**set rspan destination 1/2 901**

Configuring Multiple RSPAN Sessions

This example shows how to configure multiple RSPAN sessions. Figure 38-5 shows an RSPAN configuration; see Table 38-5 for the necessary configuration commands to configure this RSPAN session. This example is a typical scenario where the monitoring probes would be placed in the data center and source ports in the access switches (other ports in any of the switches can also be configured for RSPAN). If there is no change in the route for SPAN traffic, the destination switch and the intermediate switches need to be configured only once.

In Figure 38-5, two RSPAN sessions are used with RSPAN VLANs 901 (for probe 1) and 902 (for probe 2). The direction of traffic over trunks T1 through T6 is shown only for understanding; the direction of the trunks depends on the STP states of the respective trunks for the RSPAN VLAN(s). You need to configure the RSPAN VLANs in each of the switches for the respective RSPAN sessions. With VTP enabled in the network, you can create the RSPAN VLAN in one switch and VTP propagates it to the other switches in that VTP domain. With VTP disabled, create the RSPAN VLANs in each switch.

Figure 38-5 Configuring Multiple RSPAN Sessions

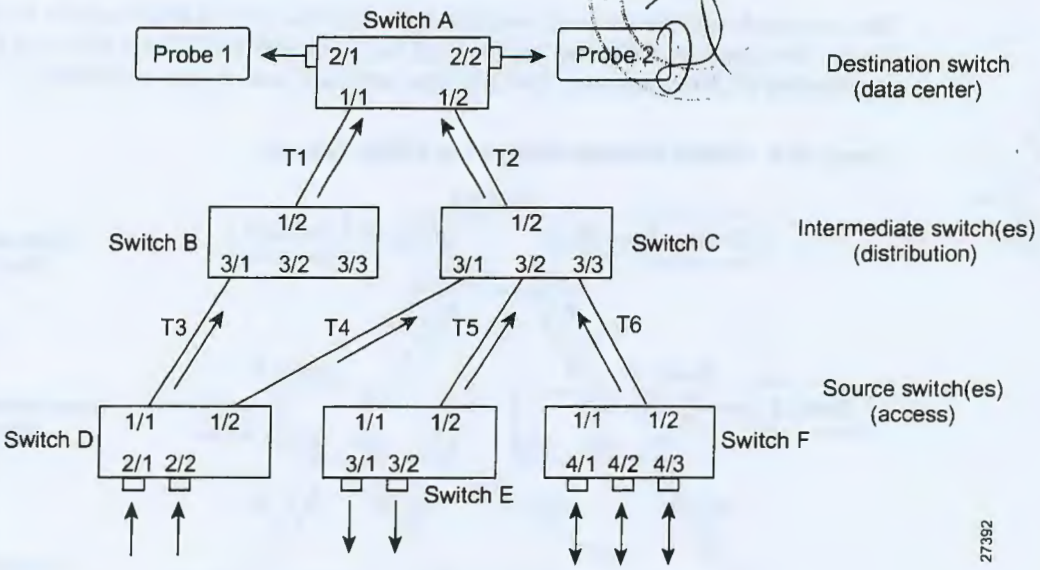


Table 38-5 Configuring Multiple RSPAN Sessions

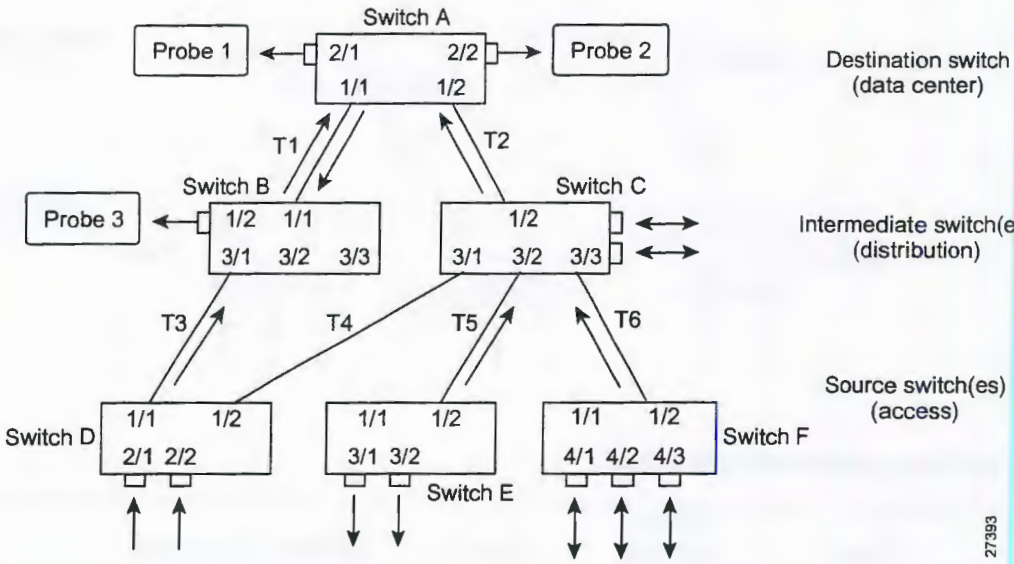
Switch	Port	RSPAN VLAN(s)	Direction	RSPAN CLI Commands
A (destination)	2/1	901	–	**set rspan destination 2/1 901**
A (destination)	2/2	902	–	**set rspan destination 2/2 902**
B (intermediate)	–	901, 902	–	No RSPAN CLI command needed
C (intermediate)	–	901, 902	–	No RSPAN CLI command needed
D (source)	2/1-2	901	Ingress	**set rspan source 2/1-2 901 rx**
E (source)	3/1-2	901	Egress	**set rspan source 3/1-2 901 tx**
F (source)	4/1-3	901	Both	**set rspan source 4/1-3 902**

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 0734
Doc: 3701

Adding Multiple Network Analyzers to an RSPAN Session

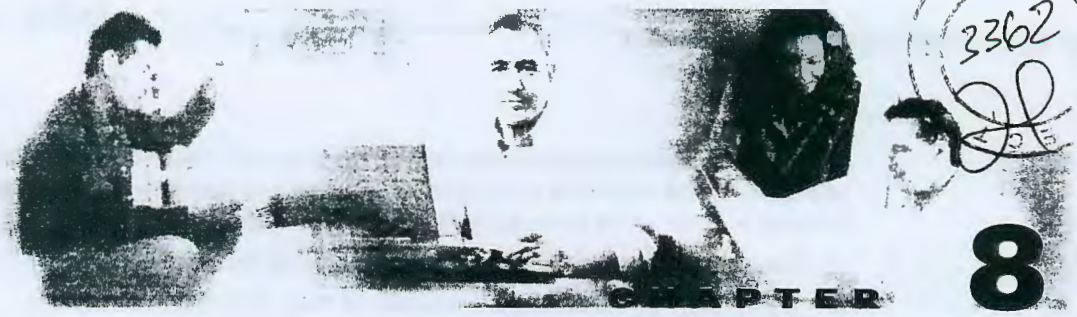
You can attach multiple network analyzers (probes) to the same RSPAN session. For example, in Figure 38-6, you can add probe 3 in Switch B to monitor RSPAN VLAN 901 using the **set rspan destination 1/2 901** command. Similarly, you could add source ports to Switch C.

Figure 38-6 Adding Multiple Probes to an RSPAN Session



Ap BP

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0735
Fls:
Doc: 3701



CHAPTER 8

Configuring Spanning Tree

This chapter describes the IEEE 802.1D bridge Spanning Tree Protocol (STP) and how to use and configure Cisco's proprietary spanning tree protocols, Per VLAN Spanning Tree + (PVST+) and Multi-Instance Spanning Tree Protocol (MISTP), on the Catalyst 6500 series switches.

Note For information on configuring the spanning tree PortFast, UplinkFast, and BackboneFast features, see Chapter 9, "Configuring Spanning Tree PortFast, UplinkFast, BackboneFast, and Loop Guard."

This chapter consists of these sections:

- Understanding How Spanning Tree Protocols Work, page 8-1
- Understanding PVST+ and MISTP Modes, page 8-10
- Understanding Bridge Identifiers, page 8-12
- Understanding How Multiple Spanning Trees Work, page 8-14
- Understanding How BPDU Skewing Works, page 8-22
- Using PVST+, page 8-23
- Using MISTP-PVST+ or MISTP, page 8-29
- Configuring a Root Switch, page 8-38
- Configuring Spanning Tree Timers, page 8-42
- Configuring Multiple Spanning Tree, page 8-44
- Configuring BPDU Skewing, page 8-56

Note For complete syntax and usage information for the commands used in this chapter, refer to the *Catalyst 6500 Series Command Reference* publication.

Understanding How Spanning Tree Protocols Work

This section describes the specific functions that are common to all spanning tree protocols. Cisco's proprietary spanning tree protocols, PVST+ and MISTP, are based on IEEE 802.1D STP. (See the "Understanding PVST+ and MISTP Modes" section on page 8-10 for information about PVST+ and MISTP.) The 802.1D STP is a Layer 2 management protocol that provides path redundancy in a network while preventing undesirable loops. All spanning tree protocols use an algorithm that calculates the best loop-free path through the network.

RQS Nº 03/2005 - CN - CPMI - CORREIOS
0756
Doc: 3701

STP uses a distributed algorithm that selects one bridge of a redundantly connected network as the root of a spanning tree connected active topology. STP assigns roles to each port depending on what the port's function is in the active topology. Port roles are as follows:

- Root—A forwarding port elected for the spanning tree topology
- Designated—A forwarding port elected for every switched LAN segment
- Alternate—A blocked port providing an alternate path to the root port in the spanning tree
- Backup—A blocked port in a loopback configuration

Switches that have ports with these assigned roles are called root or designated switches. For more information, see the "Understanding How a Switch Becomes the Root Switch" section on page 8-3.

In Ethernet networks, only one active path may exist between any two stations. Multiple active paths between stations can cause loops in the network. When loops occur, some switches recognize stations on both sides of the switch. This situation causes the forwarding algorithm to malfunction allowing duplicate frames to be forwarded.

Spanning tree algorithms provide path redundancy by defining a tree that spans all of the switches in an extended network and then forces certain redundant data paths into a standby (blocked) state. At regular intervals, the switches in the network send and receive spanning tree packets that they use to identify the path. If one network segment becomes unreachable, or if spanning tree costs change, the spanning tree algorithm reconfigures the spanning tree topology and reestablishes the link by activating the standby path.

Spanning tree operation is transparent to end stations, which do not detect whether they are connected to a single LAN segment or a switched LAN of multiple segments.

These sections describe the STP:

- Understanding How a Topology is Created, page 8-2
- Understanding How a Switch Becomes the Root Switch, page 8-3
- Understanding How Bridge Protocol Data Units Work, page 8-3
- Spanning Tree Port States, page 8-4

Understanding How a Topology is Created

All switches in an extended LAN participating in a spanning tree gather information about other switches in the network through an exchange of data messages known as bridge protocol data units (BPDUs). This exchange of messages results in the following actions:

- A unique root switch is elected for the spanning tree network topology.
- A designated switch is elected for every switched LAN segment.
- Any loops in the switched network are eliminated by placing redundant switch ports in a backup state; all paths that are not needed to reach the root switch from anywhere in the switched network are placed in STP-blocked mode.

The topology of an active switched network is determined by the following:

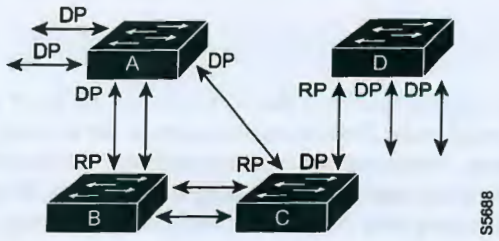
- The unique switch identifier Media Access Control ([MAC] address of the switch) associated with each switch
- The path cost to the root associated with each switch port
- The port identifier (MAC address of the port) associated with each switch port

In a switched network, the root switch is the logical center of the spanning tree topology. A spanning tree protocol uses BPDUs to elect the root switch and root port for the switched network, as well as the root port and designated port for each switched segment.

Understanding How a Switch Becomes the Root Switch

If all switches are enabled with default settings, the switch with the lowest MAC address in the network becomes the root switch. In Figure 8-1, Switch A is the root switch because it has the lowest MAC address. However, due to traffic patterns, number of forwarding ports, or line types, Switch A might not be the ideal root switch. A switch can be forced to become the root switch by increasing the priority (that is, lowering the numerical priority number) on the preferred switch. This action causes the spanning tree to recalculate the topology and make the selected switch the root switch.

Figure 8-1 Configuring a Loop-Free Topology



RP = Root Port
DP = Designated Port

You can change the priority of a port to make it the root port. When the spanning tree topology is based on default parameters, the path between source and destination stations in a switched network might not be ideal. 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.

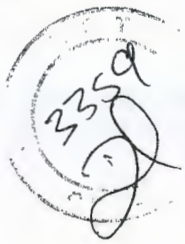
For example, assume that a port on Switch B is a fiber-optic link. Also, another port on Switch B (an unshielded twisted-pair [UTP] link) is the root port. Network traffic might be more efficient over the high-speed fiber-optic link. By changing the Port Priority parameter for the UTP port to a higher priority (lower numerical value) than the fiber-optic port, the UTP port becomes the root port. You could also accomplish this scenario by changing the Port Cost parameter for the UTP port to a lower value than that of the fiber-optic port.

Understanding How Bridge Protocol Data Units Work

BPDUs contain configuration information about the transmitting switch and its ports, including switch and port MAC addresses, switch priority, port priority, and port cost. Each configuration BPDU contains this information:

- The unique identifier of the switch that the transmitting switch believes to be the root switch
- The cost of the path to the root from the transmitting port
- The identifier of the transmitting port

RQS Nº 03/2005 - CN - CPMI - CORREIOS
0737
Fls:
Doc: 3701



The switch sends configuration BPDUs to communicate with and compute the spanning tree topology. A MAC frame conveying a BPDU sends the switch group address to the destination address field. All switches connected to the LAN on which the frame is transmitted receive the BPDU. BPDUs are not directly forwarded by the switch, but the receiving switch uses the information in the frame to calculate a BPDU and, if the topology changes, initiates a BPDU transmission.

A BPDU exchange results in the following:

- One switch is elected as the root switch.
- The shortest distance to the root switch is calculated for each switch.
- A designated switch is selected. This is the switch that is closest to the root switch through which frames will be forwarded to the root.
- A port for each switch is selected. This is the port that provides the best path from the switch to the root switch.
- Ports included in the STP are selected.

Spanning Tree Port States

Topology changes can take place in a switched network due to a link coming up or a link going down (failing). When a switch port transitions directly from nonparticipation in the topology to the forwarding state, it can create temporary data loops. Ports must wait for new topology information to propagate through the switches in the LAN before they can start forwarding frames. Also, they must allow the frame lifetime to expire for frames that have been forwarded using the old topology.

Note With Cisco IOS Release 12.1.(1)E or later on the Multilayer Switch Feature Card (MSFC), the Address Resolution Protocol (ARP) on the STP Topology Change Notification feature ensures that excessive flooding does not occur when the MSFC receives a topology change notification (TCN) from the supervisor engine. The feature causes the MSFC to send ARP requests for all the ARP entries belonging to the VLAN interface where the TCN is received. When the ARP replies come back, the Policy Feature Card (PFC) learns the MAC entries, which were lost as a result of the topology change. Learning the entries immediately following a topology change prevents excessive flooding later. There is no configuration required on the MSFC. This feature works with supervisor engine software release 5.4(2) or later.

At any given time, each port on a switch using a spanning tree protocol is in one of these states:

- Blocking
- Listening
- Learning
- Forwarding
- Disabled

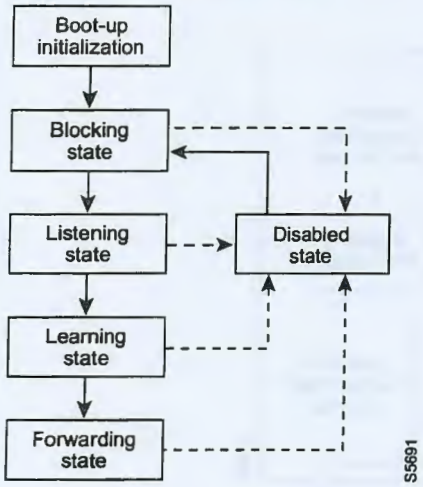
A port moves through these states as follows:

- 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 8-2 illustrates how a port moves through the states.

3388

Figure 8-2 STP Port States



You can modify each port state by using management software, for example, VLAN Trunking Protocol (VTP). When you enable spanning tree, every switch in the network goes through the blocking state and the transitory states of listening and learning at power up. If properly configured, each port stabilizes into the forwarding or blocking state.

When the spanning tree algorithm places a port in the forwarding state, the following occurs:

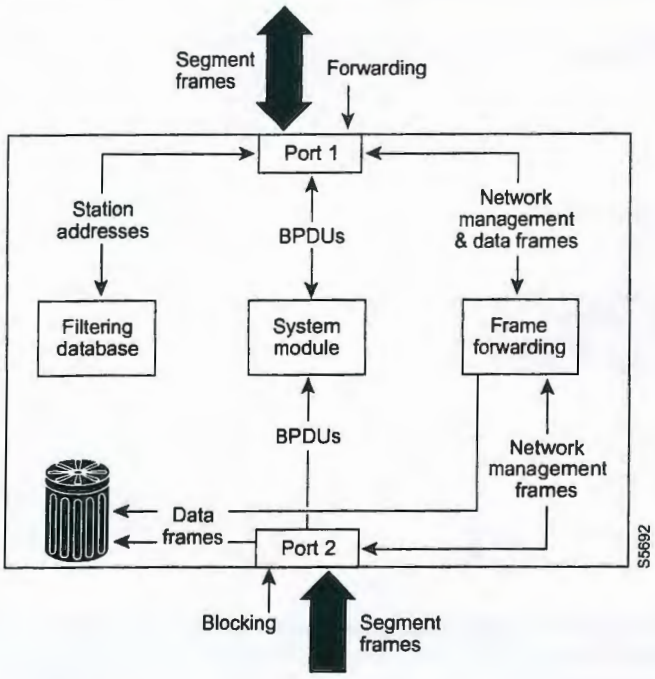
- The port is put into the listening state while it waits for protocol information that suggests it should go to the blocking state.
- The port waits for the expiration of a protocol timer that moves the port to the learning state.
- In the learning state, the port continues to block frame forwarding as it learns station location information for the forwarding database.
- The expiration of a protocol timer moves the port to the forwarding state, where both learning and forwarding are enabled.

Blocking State

A port in the blocking state does not participate in frame forwarding (see Figure 8-3). After initialization, a BPDU is sent to each port in the switch. A switch initially assumes it is the root until it exchanges BPDUs with other switches. This exchange establishes which switch in the network is really the root. If only one switch resides in the network, no exchange occurs, the forward delay timer expires, and the ports move to the listening state. A switch always enters the blocking state following switch initialization.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0738
Fls:
Doc: 3701

Figure 8-3 Port 2 in Blocking State



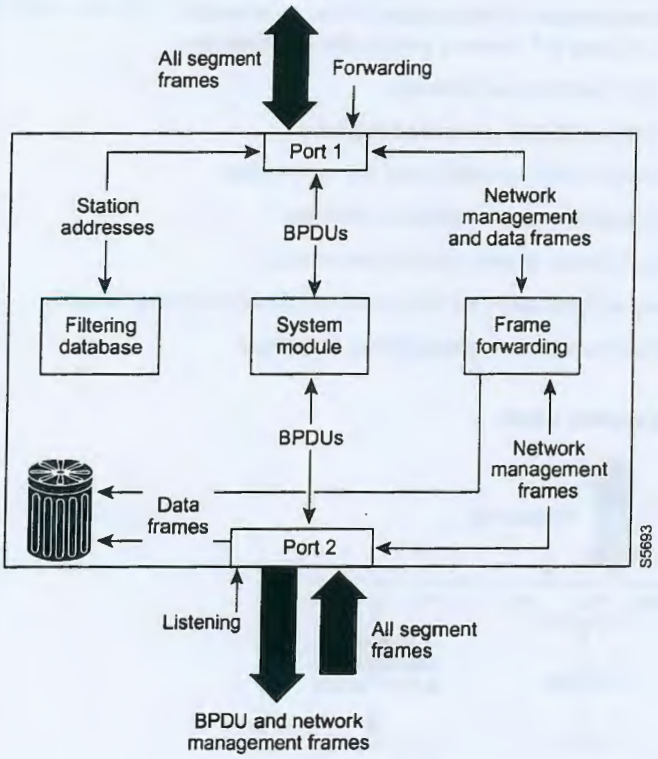
A port in the blocking state performs as follows:

- Discards frames received from the attached segment.
- Discards frames switched from another port for forwarding.
- Does not incorporate station location into its address database. (There is no learning on a blocking 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 port enters after the blocking state. The port enters this state when the spanning tree determines that the port should participate in frame forwarding. Learning is disabled in the listening state. Figure 8-4 shows a port in the listening state.

Figure 8-4 Port 2 in Listening State



A port in the listening state performs as follows:

- Discards frames received from the attached segment.
- Discards frames switched from another port for forwarding.
- Does not incorporate 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.
- Processes BPDUs received from the system module.
- Receives and responds to network management messages.

3356
RQS Nº 03/2005 - CN
CPMI - CORREIOS
0739
Fls:
Doc: 3201

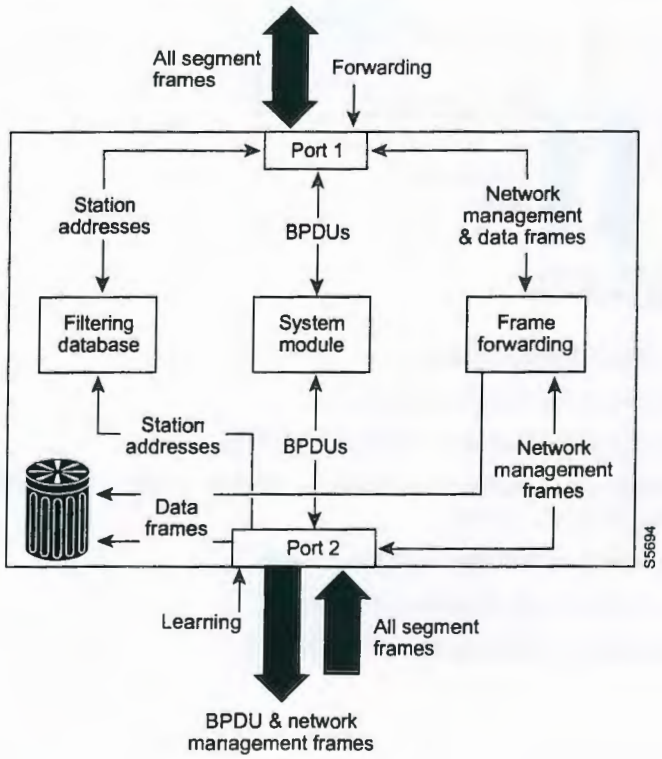
Learning State

A port in the learning state prepares to participate in frame forwarding. The port enters the learning state from the listening state. Figure 8-5 shows a port in the learning state.

A port in the learning state performs as follows:

- Discards frames received from the attached segment.
- Discards frames switched from another port for forwarding.
- Incorporates 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.

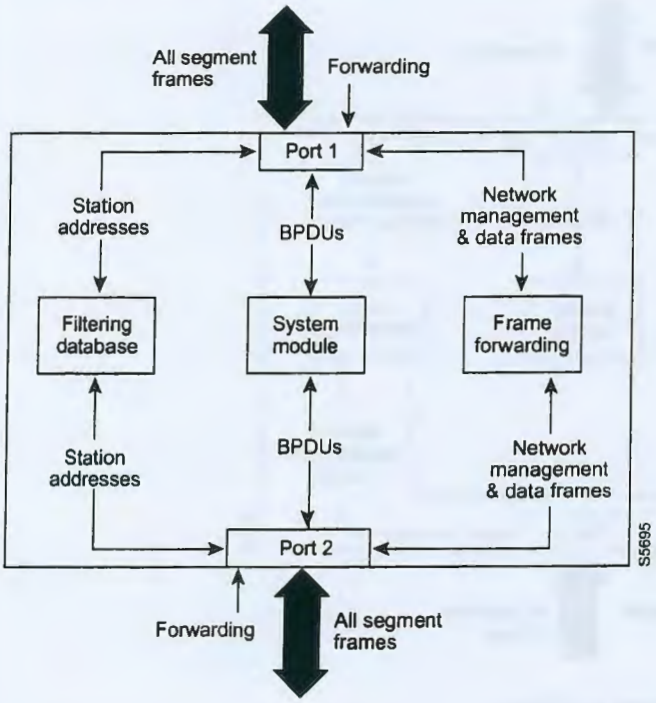
Figure 8-5 Port 2 in Learning State



Forwarding State

A port in the forwarding state forwards frames, as shown in Figure 8-6. The port enters the forwarding state from the learning state.

Figure 8-6 Port 2 in Forwarding State



A port in the forwarding state performs as follows:

- Forwards frames received from the attached segment.
- Forwards frames switched from another port for forwarding.
- Incorporates 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.

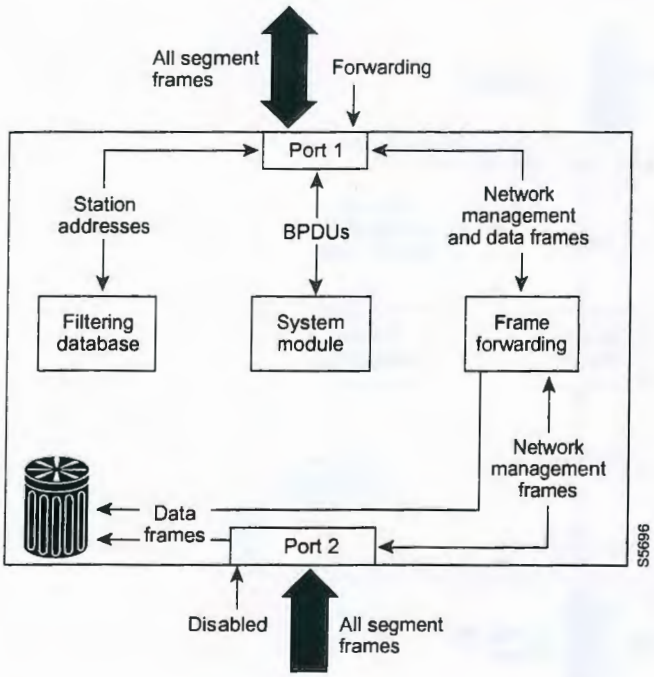
Caution Use spanning tree PortFast mode only on ports directly connected to individual workstations to allow these ports to come up and go directly to the forwarding state, instead of having to go through the entire spanning tree initialization process. To prevent illegal topologies, enable spanning tree on ports connected to switches or other devices that forward messages. For more information about PortFast, see Chapter 9, "Configuring Spanning Tree PortFast, UplinkFast, BackboneFast, and Loop Guard."

3354
RECEBIDO EM 03/2005 - CN
CPMI - CORREIOS
0740
Fls:
3701
Doc:

Disabled State

A port in the disabled state does not participate in frame forwarding or STP, as shown in Figure 8-7. A port in the disabled state is virtually nonoperational.

Figure 8-7 Port 2 in Disabled State



A disabled port performs as follows:

- Discards frames received from the attached segment.
- Discards frames switched from another port for forwarding.
- Does not incorporate station location into its address database. (There is no learning, so there is no address database update.)
- Receives BPDUs but does not direct them to the system module.
- Does not receive BPDUs for transmission from the system module.
- Receives and responds to network management messages.

Understanding PVST+ and MISTP Modes

Catalyst 6500 series switches provide two proprietary spanning tree modes based on the IEEE 802.1D standard and one mode that is a combination of the two modes:

- Per VLAN Spanning Tree (PVST+)
- Multi-Instance Spanning Tree Protocol (MISTP)
- MISTP-PVST+ (combination mode)

3352

An overview of each mode is provided in this section. Each mode is described in detail in these sections:

- Using PVST+, page 8-23
- Using MISTP-PVST+ or MISTP, page 8-29

Caution If your network currently uses PVST+ and you plan to use MISTP on any switch, you must first enable MISTP-PVST+ on the switch and configure an MISTP instance to avoid causing loops in the network.

PVST+ Mode

PVST+ is the default spanning tree protocol used on all Ethernet, Fast Ethernet, and Gigabit Ethernet port-based VLANs on Catalyst 6500 series switches. PVST+ runs on each VLAN on the switch, ensuring that each VLAN has a loop-free path through the network.

PVST+ provides Layer 2 load balancing for the VLAN on which it runs; you can create different logical topologies using the VLANs on your network to ensure that all the links are used and no link is oversubscribed.

Each PVST+ instance on a VLAN has a single root switch. This root switch propagates the spanning tree information associated with that VLAN to all other switches in the network. This process ensures that the network topology is maintained because each switch has the same knowledge about the network.

MISTP Mode

MISTP is an optional spanning tree protocol that runs on Catalyst 6500 series switches. MISTP allows you to group multiple VLANs under a single instance of spanning tree (an MISTP instance). MISTP combines the Layer 2 load-balancing benefits of PVST+ with the lower CPU load of IEEE 802.1Q.

An MISTP instance is a virtual logical topology defined by a set of bridge and port parameters. When you map VLANs to an MISTP instance, this virtual logical topology becomes a physical topology. Each MISTP instance has its own root switch and a different set of forwarding links, that is, different bridge and port parameters.

Each MISTP instance root switch propagates the information associated with it to all other switches in the network. This process maintains the network topology because it ensures that each switch has the same information about the network.

MISTP builds MISTP instances by exchanging MISTP BPDUs with peer entities in the network. MISTP uses one BPDU for each MISTP instance, rather than one for each VLAN, as in PVST+. Because there are fewer BPDUs in an MISTP network, MISTP networks converge faster with less overhead. MISTP discards PVST+ BPDUs.

An MISTP instance can have any number of VLANs mapped to it, but a VLAN can be mapped only to a single MISTP instance. You can easily move a VLAN (or VLANs) in an MISTP topology to another MISTP instance if it has converged. (However, if ports are added at the same time the VLAN is moved, convergence time is required.)

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0741
Fls:
3701
Doc:

MISTP-PVST+ Mode

MISTP-PVST+ is a transition spanning tree mode that allows you to use the MISTP functionality on Catalyst 6500 series switches while continuing to communicate with Catalyst 5000 and 6500 series switches in your network that use PVST+. A switch using PVST+ mode that is connected to a switch using MISTP mode cannot see the BPDUs of the other switch, a condition that can cause loops in the network. MISTP-PVST+ allows interoperability between PVST+ and pure MISTP because it sees the BPDUs of both modes. To convert your network to MISTP, use MISTP-PVST+ to transition the network from PVST+ to MISTP.

Because MISTP-PVST+ conforms to the limits of PVST+, you cannot configure more VLAN ports on your MISTP-PVST+ switches than on your PVST+ switches.

Understanding Bridge Identifiers

These sections explain how MAC addresses are used in PVST+ and MISTP as unique bridge identifiers:

- MAC Address Allocation, page 8-12
- MAC Address Reduction, page 8-12

MAC Address Allocation

Catalyst 6500 series switches have a pool of 1024 MAC addresses that can be used as bridge identifiers for VLANs running under PVST+ or for MISTP instances. You can use the **show module** command to view the MAC address range.

MAC addresses are allocated sequentially, with the first MAC address in the range assigned to VLAN 1, the second MAC address in the range assigned to VLAN 2, and so on. The last MAC address in the range is assigned to the supervisor engine in-band (sc0) management interface.

For example, if the MAC address range is 00-e0-1e-9b-2e-00 to 00-e0-1e-9b-31-ff, the VLAN 1 bridge ID is 00-e0-1e-9b-2e-00, the VLAN 2 bridge ID is 00-e0-1e-9b-2e-01, the VLAN 3 bridge ID is 00-e0-1e-9b-2e-02, and so forth. The in-band (sc0) interface MAC address is 00-e0-1e-9b-31-ff.

MAC Address Reduction

For Catalyst 6500 series switches that support 4096 VLANs, MAC address reduction allows up to 4096 VLANs running under PVST+ or 16 MISTP instances to have unique identifiers without increasing the number of MAC addresses required on the switch. MAC address reduction reduces the number of MAC addresses required by the STP from one per VLAN or MISTP instance to one per switch. However, because VLANs running under PVST+ and MISTP instances running under MISTP-PVST+ or MISTP are considered logical bridges, each bridge must have its own unique identifier in the network.

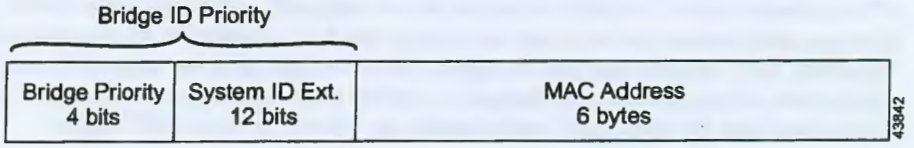
When you enable MAC address reduction, the bridge identifier stored in the spanning tree BPDU contains an additional field called the *system ID extension*. Combined with the bridge priority, the system ID extension functions as the unique identifier for a VLAN or an MISTP instance. The system ID extension is always the number of the VLAN or the MISTP instance; for example, the system ID extension for VLAN 100 is 100, and the system ID extension for MISTP instance 2 is 2.

Figure 8-8 shows the bridge identifier when you do not enable MAC address reduction. The bridge identifier consists of the bridge priority and the MAC address.

Figure 8-8 Bridge Identifier without MAC Address Reduction

Figure 8-9 shows the bridge identifier when you enable MAC address reduction. The bridge identifier consists of the bridge priority, the system ID extension, and the MAC address. The bridge priority and the system ID extension combined are known as the *bridge ID priority*. The bridge ID priority is the unique identifier for the VLAN or the MISTP instance.

Figure 8-9 Bridge Identifier with MAC Address Reduction Enabled



When you enter a **show spantree** command, you can see the bridge ID priority for a VLAN in PVST+ or for an MISTP instance in MISTP or MISTP-PVST+ mode.

This example shows the bridge ID priority for VLAN 1 when you enable MAC address reduction in PVST+ mode. The unique identifier for this VLAN is 32769.

```
Console> (enable) show spantree 1
VLAN 1
Spanning tree mode          PVST+
Spanning tree type          ieee
  .
  .
  .
Bridge ID MAC ADDR          00-d0-00-4c-18-00
Bridge ID Priority          32769  (bridge priority: 32768, sys ID ext: 1)
Bridge Max Age 20 sec   Hello Time 2  sec   Forward Delay 15 sec
```

If you have a Catalyst switch in your network with MAC address reduction enabled, you should also enable MAC address reduction on all other Layer-2 connected switches to avoid undesirable root 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.

Therefore, if another bridge in the same spanning-tree domain does not run the MAC address reduction feature, it could claim and win root bridge ownership because of the finer granularity in the selection of its bridge ID.

Note The MAC address reduction feature is enabled by default on Cisco switches that have 64 MAC addresses (Cisco 7606, CISCO7603, WS-C6503, and WS-C6513).

RQS Nº 03/2005 - CN - CPMI - CORREIOS
Fls: 0742
Doc: 3701

Understanding How Multiple Spanning Trees Work

The Multiple Spanning Tree (MST) feature is an upcoming (as of this software release) IEEE standard. 802.1s for MST is an amendment to 802.1Q. MST extends the 802.1w Rapid Spanning Tree (RST) algorithm to multiple spanning trees. This extension provides for both rapid convergence and load balancing in a VLAN environment. For a given topology, MST converges faster than PVST+ and MISTP. The MST feature for this release is based on a draft version of the IEEE standard. MST is backward compatible with 802.1D STP, 802.1w, the Rapid Spanning Tree Protocol (RSTP), and the Cisco PVST+ architecture.

MST allows you to build multiple spanning trees over VLAN 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, having different VLAN-spanning tree instance assignments located in different parts of the network makes it easier to administrate and optimally utilize redundant paths. However, a spanning tree instance can exist only on bridges that have compatible VLAN-instance assignments. Therefore, MST requires that you configure a set of bridges with the same MST configuration information, allowing them to participate in a given 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 a variant of STP (IST) that 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 encompasses the whole bridged domain. The MST region appears as a virtual bridge to adjacent SST bridges and MST regions.
  - The collection of ISTs in each MST region, the CST that interconnects the MST regions, and the SST bridges define Common and Internal Spanning Tree (CIST). 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 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 given 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 part of 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 behave as if MAC reduction is enabled.
  - For private VLANs (PVLANs), secondary VLANs are mapped to the same instance as the primary.

Follow these guidelines when using MST:

- Do not disable spanning tree on any VLAN in any of the PVST bridges.
- Ensure that all PVST spanning tree root bridges have lower (numerically higher) priority than the CST root bridge.
- Do not use PVST bridges as the root of CST.
- Ensure that trunks carry all of the VLANs mapped to an instance or do not carry any VLANs at all.
- 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 carried out during the maintenance window. This action should be taken because the complete MST database gets re-initialized for any incremental changes (such as adding new VLANs to instances or moving VLANs across instances).

These sections describe MST:

- Rapid Spanning Tree Protocol, page 8-15
- MST-to-SST Interoperability, page 8-17
- Common Spanning Tree, page 8-18
- MST Instances, page 8-18
- MST Configuration, page 8-18
- MST Region, page 8-19
- Message Age and Hop Count, page 8-20
- MST-to-PVST+ Interoperability, page 8-21

Rapid Spanning Tree Protocol

RSTP significantly reduces the time to reconfigure the active topology of the network when changes to the physical topology or its configuration parameters occur. 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 through an explicit handshake between them. RSTP allows switch port configuration so the ports can transition to forwarding directly when the switch reinitializes.

3348
DEL-LAN-05/2005-CN
CORREIOS
Fls: 0743
Doc: 3201

RSTP, specified in 802.1w, supersedes STP specified in 802.1D, while remaining compatible with STP. RSTP provides the structure on which the MST operates. You configure RSTP when you configure the MST feature. For more information, see the "Configuring Multiple Spanning Tree" section on page 8-44.

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. RSTP BPDUs are not visible on the port; only version 3 BPDUs are visible.
- 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 8-1 provides a comparison between STP port states and RSTP port states.

Table 8-1 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

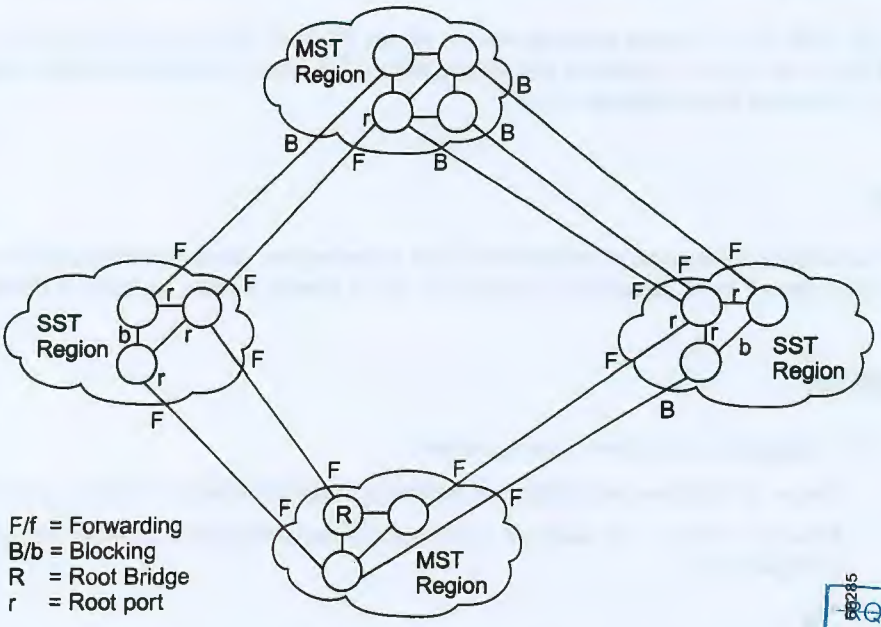
1. IEEE 802.1D port state designation.
2. IEEE 802.1w port state designation. Discarding is the same as blocking in MST.

In a stable topology, RSTP ensures that every root port and designated port transition to forwarding while all alternate ports and backup ports are always in the discarding state.

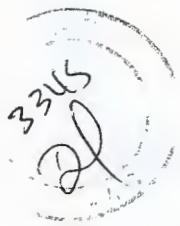
MST-to-SST Interoperability

A virtual bridged LAN may contain interconnected regions of SST and MST bridges. Figure 8-10 shows this relationship.

Figure 8-10 Network with Interconnected SST and MST Regions



ECT-QS Nº 03/2005 - CN
CPMI - CORREIOS
0744
Fls:
Doc: 3701



To the spanning tree protocol running in the SST region, an MST region appears as a single SST or pseudobridge. 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.

Common Spanning Tree

CST (802.1Q) is a single spanning tree for all the VLANs. In a Catalyst 6500 series switch running PVST+, the VLAN 1 spanning tree corresponds to CST. In a Catalyst 6500 series 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 optional.

MST Configuration

MST configuration has three parts as follows:

- Name—A 32-character string (null padded and null terminated) 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 the MST configuration is committed.

3344

- 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 treated as an SST BPDU.

When you modify an MST configuration through either a console or Telnet connection, the session exits without committing those changes and the edit buffer locks. Further configuration is impossible until you discard the existing edit buffer and acquire a new edit buffer by entering the **set spantree mst config rollback force** command.

MST Region

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 certain 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 mechanism assigns a port role to the boundary and the same state as that of the IST port. The IST port at the boundary can take up any port role except a backup port role.

ROS Nº 03/2005 - CN
CPMI - CORREIOS
0745
Fls:
Doc: 3701

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. Enter the **show spantree mst** command to display the information about the IST master, path cost, and remaining hops for the bridge.

Edge Ports

A port that is connected to a nonbridging device (for example, a host or a router) is an edge port. 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.

Note To configure a port as an edge port, you enable PortFast on that port. When you enter the **show spantree portfast** *mod/port* command, if the designation for a port is displayed as edge, that port is also a PortFast port. For more information see Chapter 9, "Configuring Spanning Tree PortFast, UplinkFast, BackboneFast, and Loop Guard."

To prevent a misconfiguration, the PortFast operation is turned off if the port receives a BPDU. You can display the configured and operational status of Portfast by using the **show spantree mst** *mod/port* 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 **set spantree mst link-type** 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 mechanism that is very similar to the IP TTL mechanism. 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

3342
21

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 the 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.

MST-to-PVST+ Interoperability

These guidelines apply in a topology where you configure MST switches (all in the same region) to interact with PVST+ switches that have VLANs 1—100 set up to span throughout the network:

- Configure the root for all VLANs inside the MST region. The ports that belong to the MST switch at the boundary simulate PVST+ and send PVST+ BPDUs for all the VLANs. This example shows the ports simulating PVST:

```
Console> (enable) show spantree mst 3
Spanning tree mode          MST
Instance                    3
VLANs Mapped:               31-40

Designated Root             00-10-7b-bb-2f-00
Designated Root Priority    8195  (root priority:8192, sys ID ext:3)
Designated Root Cost        0          Remaining Hops 20
Designated Root Port        1/0

Bridge ID MAC ADDR          00-10-7b-bb-2f-00
Bridge ID Priority          8195  (bridge priority:8192, sys ID ext:3)

Port                    State         Role Cost     Prio Type
----------------------- ------------- ---- -------- ------------------------
 6/1                    forwarding    BDRY    10000   30 P2P,
Boundary(PVST)
 6/2                    blocking      BDRY    20000   32 P2P,
Boundary(PVST)
```

  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.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0746
Fls:
3701
Doc:

Understanding How BPDU Skewing Works

BPDU skewing is the difference in time between when the BPDUs are expected to be received by the switch and when the BPDUs are actually received by that switch. Skewing occurs as follows:

- Spanning tree timers lapse.
- Expected BPDUs are not received by the switch.
- Spanning tree detects topology changes.

The skew causes BPDUs to reflood the network to keep the spanning tree topology database current.

The root switch advertises its presence by sending out BPDUs for the configured hello time interval. The nonroot switches receive and process one BPDU during each configured time period. A VLAN may not receive the BPDU as scheduled. If the BPDU is not received on a VLAN at the configured time interval, the BPDU is skewed.

Spanning tree uses the hello time (see the "Configuring the Hello Time" section on page 8-43) to detect when a connection to the root switch exists through a port and when that connection is lost. This feature applies to both PVST+ and MISTP. In MISTP, the skew detection is on a per-instance basis.

BPDU skewing detects BPDUs that are not processed in a regular time frame on the nonroot switches in the network. If BPDU skewing occurs, a syslog message is displayed. The syslog applies to both PVST+ and MISTP.

The number of syslog messages that are generated may impact the network convergence and the CPU utilization of the switch. New syslog messages are not generated as individual messages for every VLAN because the higher the number of syslog messages that are reported, the slower the switching process will be. To reduce the impact on the switch, the syslog messages are as follows:

- Generated 50 percent of the maximum age time (see the "Configuring the Maximum Aging Time" section on page 8-44)
- Rate limited at one for every 60 seconds

Using PVST+

PVST+ is the default spanning tree mode for Catalyst 6500 series switches. These sections describe how to configure PVST+ on Ethernet VLANs:

- Default PVST+ Configuration, page 8-23
- Setting the PVST+ Bridge ID Priority, page 8-24
- Configuring the PVST+ Port Cost, page 8-25
- Configuring the PVST+ Port Priority, page 8-26
- Configuring the PVST+ Default Port Cost Mode, page 8-26
- Configuring the PVST+ Port Cost for a VLAN, page 8-27
- Configuring the PVST+ Port Priority for a VLAN, page 8-28
- Disabling the PVST+ Mode on a VLAN, page 8-28

Default PVST+ Configuration

Table 8-2 shows the default PVST+ configuration.

Table 8-2 PVST+ Default Configuration

Feature	Default Value
VLAN 1	All ports assigned to VLAN 1
Enable state	PVST+ enabled for all VLANs
MAC address reduction	Disabled
Bridge priority	32768
Bridge ID priority	32769 (bridge priority plus system ID extension of VLAN 1)
Port priority	32
Port cost	• Gigabit Ethernet: 4 • Fast Ethernet: 19[1] • FDDI/CDDI: 10 • Ethernet: 100[2]
Default spantree port cost mode	Short (802.1D)
Port VLAN priority	Same as port priority but configurable on a per-VLAN basis in PVST+
Port VLAN cost	Same as port cost but configurable on a per-VLAN basis in PVST+
Maximum aging time	20 seconds
Hello time	2 seconds
Forward delay time	15 seconds

1. If 10/100 Mbps ports autonegotiate or are hard set to 100 Mbps, the port cost is 19.
2. If 10/100 Mbps ports autonegotiate or are hard set to 10 Mbps, the port cost is 100.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 0747
Doc: 3701

Setting the PVST+ Bridge ID Priority

The bridge ID priority is the priority of a VLAN when the switch is in PVST+ mode.

When the switch is in PVST+ mode without MAC address reduction enabled, you can enter a bridge priority value between 0–65535. The bridge priority value you enter also becomes the VLAN bridge ID priority for that VLAN.

When the switch is in PVST+ mode with MAC address reduction enabled, you can enter one of 16 bridge priority values: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, or 61440.

The bridge priority is combined with the system ID extension (that is, the ID of the VLAN) to create the bridge ID priority for the VLAN.

To set the spanning tree bridge priority for a VLAN, perform this task in privileged mode:

	Task	Command
Step 1	Set the PVST+ bridge ID priority for a VLAN.	**set spantree priority** *bridge_ID_priority* [*vlan*]
Step 2	Verify the bridge ID priority.	**show spantree** [*vlan*] **[active]**

This example shows how to set the PVST+ bridge ID priority when MAC address reduction is not enabled (default):

```
Console> (enable) set spantree priority 30000 1
Spantree 1 bridge priority set to 30000.
Console> (enable) show spantree 1
VLAN 1
Spanning tree mode          PVST+
Spanning tree type          ieee
Spanning tree enabled

Designated Root             00-60-70-4c-70-00
Designated Root Priority    16384
Designated Root Cost        19
Designated Root Port        2/3
Root Max Age   14 sec   Hello Time 2 sec   Forward Delay 10 sec

Bridge ID MAC ADDR          00-d0-00-4c-18-00
Bridge ID Priority          30000
Bridge Max Age 20 sec   Hello Time 2 sec   Forward Delay 15 sec

Port                     Vlan Port-State    Cost      Prio Portfast Channel_id
------------------------ ---- ------------ --------- ---- -------- ----------
 1/1                     1    not-connected          4   32 disabled 0
 1/2                     1    not-connected          4   32 disabled 0
 2/1                     1    not-connected        100   32 disabled 0
 2/2                     1    not-connected        100   32 disabled 0
```

This example shows how to set the PVST+ bridge ID priority when MAC reduction is enabled:

```
Console> (enable) set spantree priority 32768 1
Spantree 1 bridge ID priority set to 32769
(bridge priority: 32768 + sys ID extension: 1)
Console> (enable) show spantree 1/1 1
VLAN 1
Spanning tree mode          PVST+
Spanning tree type          ieee
Spanning tree enabled
```

```
Designated Root             00-60-70-4c-70-00
Designated Root Priority    16384
Designated Root Cost        19
Designated Root Port        2/3
Root Max Age   14 sec   Hello Time 2 sec   Forward Delay 10 sec

Bridge ID MAC ADDR          00-d0-00-4c-18-00
Bridge ID Priority          32769 (bridge priority: 32768, sys ID ext: 1)
Bridge Max Age 20 sec   Hello Time 2 sec   Forward Delay 15 sec

Port                     Vlan Port-State    Cost      Prio Portfast Channel_id
------------------------ ---- ------------ --------- ---- -------- ----------
 1/1                     1    not-connected         4   32 disabled 0
 1/2                     1    not-connected         4   32 disabled 0
 2/1                     1    not-connected       100   32 disabled 0
 2/2                     1    not-connected       100   32 disabled 0
```

Configuring the PVST+ Port Cost

You can configure the port cost of switch ports. Ports with lower port costs are more likely to be chosen to forward frames. Assign lower numbers to ports attached to faster media (such as full duplex) and higher numbers to ports attached to slower media.The possible range of *cost* is 1 to 65535. The default differs for different media. Path cost is typically 1000 LAN speed in megabits per second.

To configure the PVST+ port cost for a port, perform this task in privileged mode:

	Task	Command
Step 1	Configure the PVST+ port cost for a switch port.	**set spantree portcost** {*mod/port*} *cost*
Step 2	Verify the port cost setting.	**show spantree** *mod/port*

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 "Setting the EtherChannel Port Path Cost" section in Chapter 6, "Configuring EtherChannel," for information on using the **set spantree channelcost** command.

This example shows how to configure the PVST+ port cost on a port and verify the configuration:

```
Console> (enable) set spantree portcost 2/3 12
Spantree port 2/3 path cost set to 12.
Console> (enable) show spantree 2/3
VLAN 1
   .
   .
   .
Port                     Vlan Port-State    Cost      Prio Portfast Channel_id
------------------------ ---- ------------ --------- ---- -------- ----------
 1/1                     1    not-connected         4   32 disabled 0
 1/2                     1    not-connected         4   32 disabled 0
 2/1                     1    not-connected       100   32 disabled 0
 2/2                     1    not-connected       100   32 disabled 0
 2/3                     1    forwarding           12   32 disabled 0
 2/4                     1    not-connected       100   32 disabled
```

Configuring the PVST+ Port Priority

You can configure the port priority of switch ports in PVST+ mode. The port with the lowest priority value forwards frames for all VLANs. The possible port priority value is a multiple of 16 from 0 to 240. The default is 32. If all ports have the same priority value, the port with the lowest port number forwards frames.

To configure the PVST+ port priority for a port, perform this task in privileged mode:

	Task	Command
Step 1	Configure the PVST+ port priority for a switch port.	**set spantree portpri** *mod/port priority*
Step 2	Verify the port priority setting.	**show spantree** *mod/port*

This example shows how to configure the PVST+ port priority for a port:

```
Console> (enable) set spantree portpri 2/3 48
Bridge port  2/3 port priority set to 48.
Console> (enable) show spantree 2/3
VLAN 1
   .
   .
   .
Port                     Vlan Port-State    Cost      Prio Portfast Channel_id
------------------------ ---- ------------ --------- ---- -------- ----------
 1/1                     1    not-connected         4   32 disabled 0
 1/2                     1    not-connected         4   32 disabled 0
 2/1                     1    not-connected       100   32 disabled 0
 2/2                     1    not-connected       100   32 disabled 0
 2/3                     1    forwarding           19   48 disabled 0
 2/4                     1    not-connected       100   32 disabled 0
```

This example shows that values that are not multiples of 16 (between the values of 0 to 63) are converted to the nearest multiple of 16:

```
Console> (enable) set spantree portpri 2/3 2
Vlan port priority must be one of these numbers:0, 16, 32, 48, 64, 80,
96, 112, 128, 144,
160, 176, 192, 208, 224, 240
converting 2 to 0 nearest multiple of 16
Bridge port  2/3 port priority set to 0.
```

Configuring the PVST+ Default Port Cost Mode

If any switch in your network is using a port speed of 10 Gb or over and the network is using PVST+ spanning tree mode, all switches in the network must have the same path cost defaults. You can enter the **set spantree defaultcostmode** command to force all VLANs associated with all the ports to have the same port cost default set.

Two default port cost modes are available—short and long.

- The short mode has these parameters:
  - Portcost
  - Portvlancost
  - When uplinkfast is enabled, the actual cost is incremented by 3000

- The long mode has these parameters:
  - Portcost
  - Portvlancost
  - When uplinkfast is enabled, the actual cost is incremented by 10,000,000
  - EtherChannel computes the cost of a bundle using the formula, AVERAGE_COST/NUM_PORT

The default port cost mode is set to short in PVST+ mode. For port speeds of 10 Gb and greater, the default port cost mode must be set to long.

To configure the PVST+ default port cost mode, perform this task in privileged mode:

Task	Command
Configure the PVST+ default port cost mode.	**set spantree defaultcostmode** {**short** | **long**}

This example shows how to configure the PVST+ default port cost mode:

```
Console> (enable) set spantree defaultcostmode long
Portcost and portvlancost set to use long format default values.
Console> (enable)
```

Configuring the PVST+ Port Cost for a VLAN

You can configure the port cost for a port on a per-VLAN basis. Ports with a lower port cost in the VLAN are more likely to be chosen to forward frames. You should assign lower numbers to ports attached to faster media (such as full duplex) and higher numbers to ports attached to slower media. The default cost differs for different media.

You can set a cost value from 1 to 65535.

To configure the PVST+ port VLAN cost for a port, perform this task in privileged mode:

Task	Command
Configure the PVST+ port cost for a VLAN on a port.	**set spantree portvlancost** {*mod/port*} [**cost** *cost*] [*vlan_list*]

Note When you use 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 "Setting the EtherChannel Port Path Cost" section in Chapter 6, "Configuring EtherChannel," for information on using the **set spantree channelcost** command.

This example shows how to configure the PVST+ port VLAN cost on port 2/3 for VLANs 1 through 5:

```
Console> (enable) set spantree portvlancost 2/3 cost 20000 1-5
Port 2/3 VLANs 6-11,13-1005,1025-4094 have path cost 12.
Port 2/3 VLANs 1-5,12 have path cost 20000.
This parameter applies to trunking ports only.
Console> (enable
```

ROS Nº 03/2005 - CN
CPMI - CORREIOS
0749
Fls:
3701
Doc:

Configuring the PVST+ Port Priority for a VLAN

When the switch is in PVST+ mode, you can set the port priority for a trunking port in a VLAN. The port with the lowest priority value for a specific VLAN forwards frames for that VLAN. The possible port priority value is a multiple of 16 from 0 to 240. The default is 16. If all ports have the same priority value for a particular VLAN, the port with the lowest port number forwards frames for that VLAN.

The port VLAN priority value must be lower than the port priority value.

To configure the port VLAN priority for a port, perform this task in privileged mode:

	Task	Command
Step 1	Configure the PVST+ port priority for a VLAN on a port.	**set spantree portvlanpri** *mod/port priority* [*vlans*]
Step 2	Verify the port VLAN priority.	**show config all**

This example shows how to configure the port priority for VLAN 6 on port 2/3:

```
Console> (enable) set spantree portvlanpri 2/3 16 6
Port 2/3 vlans 6 using portpri 16.
Port 2/3 vlans 1-5,7-800,802-1004,1006-4094 using portpri 32.
Port 2/3 vlans 801,1005 using portpri 4.
This parameter applies to trunking ports only.
Console> (enable) show config all
    .
    .
    .
set spantree portcost    2/12,2/15 19
set spantree portcost    2/1-2,2/4-11,2/13-14,2/16-48 100
set spantree portcost    2/3 12
set spantree portpri     2/1-48 32
set spantree portvlanpri 2/1 0
set spantree portvlanpri 2/2 0
    .
    .
    .
set spantree portvlanpri 2/48 0
set spantree portvlancost 2/1 cost 99
set spantree portvlancost 2/2 cost 99
set spantree portvlancost 2/3 cost 20000 1-5,12
```

Disabling the PVST+ Mode on a VLAN

When the switch is in PVST+ mode, you can disable spanning tree on individual VLANs or all VLANs. When you disable spanning tree on a VLAN, the switch does not participate in spanning tree and any BPDUs received in that VLAN are flooded on all ports.

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.

Caution Do not disable spanning tree on a VLAN unless all switches or routers in the VLAN have spanning tree disabled. You cannot disable spanning tree on some switches or routers in a VLAN and leave spanning tree enabled on other switches or routers in the VLAN. If spanning tree remains enabled on the switches and routers, they will have incomplete information about the physical topology of the network. This situation may cause unexpected results.

To disable PVST+, perform this task in privileged mode:

Task	Command
Disable PVST+ mode on a VLAN.	**set spantree disable** *vlans* **[all]**

This example shows how to disable PVST+ on a VLAN:

```
Console> (enable) set spantree disable 4
Spantree 4 disabled.
Console> (enable)
```

Using MISTP-PVST+ or MISTP

The default spanning tree mode on the Catalyst 6500 series switches is PVST+. If you want to use MISTP mode in your network, we recommend you carefully follow the procedures described in the following sections in order to avoid losing connectivity in your network.

When you change the spanning tree mode, the current mode stops, the information collected at runtime is used to build the port database for the new mode, and the new spanning tree mode restarts the computation of the active topology. Information about the port states is lost; however, all of the configuration parameters are preserved for the previous mode. If you return to the previous mode, the configuration is still there.

Note We recommend that if you use MISTP mode, you should configure *all* of your Catalyst 6500 series switches to run MISTP.

To use MISTP mode, you first enable an MISTP instance and then map at least one VLAN to the instance. You must have at least one forwarding port in the VLAN in order for the MISTP instance to be active.

Note Map VLANs to MISTP instances on Catalyst 6500 series switches that are either in VTP server mode or transparent mode only. You cannot map VLANs to MISTP instances on switches that are in VTP client mode.

If you are changing a switch from PVST+ mode to MISTP mode and you have other switches in the network that are using PVST+, you must first enable MISTP-PVST+ mode on each switch on which you intend to use MISTP so that PVST+ BPDUs can flow through the switches while you configure them.

When all switches in the network are configured in MISTP-PVST+, you can then enable MISTP on all of the switches.

3334
RQS Nº 03/2005 - CN
CPMI - CORREIOS
0750
Fls:
3701
Doc:

These sections describe how to use MISTP-PVST+ or MISTP:

- Default MISTP and MISTP-PVST+ Configuration, page 8-30
- Setting the MISTP-PVST+ Mode or the MISTP Mode, page 8-30
- Configuring an MISTP Instance, page 8-32
- Mapping VLANs to an MISTP Instance, page 8-36
- Disabling MISTP-PVST+ or MISTP, page 8-38

Default MISTP and MISTP-PVST+ Configuration

Table 8-3 shows the default MISTP and MISTP-PVST+ configuration.

Table 8-3 MISTP and MISTP-PVST+ Default Configuration

Feature	Default Value
Enable state	Disabled until a VLAN is mapped to an MISTP instance
MAC address reduction	Disabled
Bridge priority	32768
Bridge ID priority	32769 (bridge priority plus the system ID extension of MISTP instance 1)
Port priority	32 (global)
Port cost	• Gigabit Ethernet: 4 • Fast Ethernet: 19[1] • FDDI/CDDI: 10 • Ethernet: 100[2]
Default port cost mode	Short (802.1D)
Port VLAN priority	Same as port priority but configurable on a per-VLAN basis in PVST+
Port VLAN cost	Same as port cost but configurable on a per-VLAN basis in PVST+
Maximum aging time	20 seconds
Hello time	2 seconds
Forward delay time	15 seconds

1. If 10/100-Mbps ports autonegotiate or are hard set to 100 Mbps, the port cost is 19.
2. If 10/100-Mbps ports autonegotiate or are hard set to 10 Mbps, the port cost is 100.

Setting the MISTP-PVST+ Mode or the MISTP Mode

If you enable MISTP in a PVST+ network, you must be careful to avoid bringing down the network. This section explains how to enable MISTP or MISTP-PVST+ on your network.

Caution If you have more than 6000 VLAN ports configured on your switch, changing from MISTP to either PVST+ or MISTP-PVST+ mode could bring down your network. Reduce the number of configured VLAN ports on your switch to no more than 6000 to avoid losing connectivity.

3332

Caution If you are working from a Telnet connection to your switch, the first time you enable MISTP-PVST+ or MISTP mode, you must do so from the switch console; do not use a Telnet connection through the data port or you will lose your connection to the switch. After you map a VLAN to an MISTP instance, you can Telnet to the switch.

To change from PVST+ to MISTP-PVST+ or MISTP, perform this task in privileged mode:

Task	Command
Set a spanning tree mode.	**set spantree mode** {**mistp** | **pvst+** | **mistp-pvst+**}

This example shows how to set a switch to MISTP-PVST+ mode:

```
Console> (enable) set spantree mode mistp-pvst+
PVST+ database cleaned up.
Spantree mode set to MISTP-PVST+.
Warning!! There are no VLANs mapped to any MISTP instance.
Console> (enable)
```

You can display VLAN-to-MISTP instance mapping information propagated from the root switch at runtime. This display is available only in the MISTP or MISTP-PVST+ mode. When in the PVST+ mode, use the optional keyword **config** to display the list of mappings configured on the local switch.

Note MAC addresses are not displayed when you specify the keyword **config**.

To display spanning tree mapping, perform this task in privileged mode:

	Task	Command
Step 1	Set the spanning tree mode to MISTP.	**set spantree mode mistp**
Step 2	Show the spanning tree mapping.	**show spantree mapping** [**config**]

This example shows how to display the spanning tree VLAN instance mapping in MISTP mode:

```
MISTP/MISTP-PVST+
Console> (enable) set spantree mode mistp
PVST+ database cleaned up.
Spantree mode set to MISTP.
Console> (enable) show spantree mapping
Inst Root Mac          Vlans
---- ----------------- --------------------------
1    00-50-3e-78-70-00 1
2    00-50-3e-78-70-00 -
3    00-50-3e-78-70-00 -
4    00-50-3e-78-70-00 -
5    00-50-3e-78-70-00 -
6    00-50-3e-78-70-00 -
7    00-50-3e-78-70-00 -
8    00-50-3e-78-70-00 -
9    00-50-3e-78-70-00 -
10   00-50-3e-78-70-00 -
11   00-50-3e-78-70-00 -
```

ROS Nº 03/2005 - CN
CPMI - CORREIOS
0751
Fls:
Doc: 3701

```
12    00-50-3e-78-70-00 -
13    00-50-3e-78-70-00 -
14    00-50-3e-78-70-00 -
15    00-50-3e-78-70-00 -
16    00-50-3e-78-70-00 -
```

Configuring an MISTP Instance

These sections describe how to configure MISTP instances:

- Configuring the MISTP Bridge ID Priority, page 8-32
- Configuring the MISTP Port Cost, page 8-33
- Configuring the MISTP Port Priority, page 8-33
- Configuring the MISTP Port Instance Cost, page 8-34
- Configuring the MISTP Port Instance Priority, page 8-34

Configuring the MISTP Bridge ID Priority

You can set the bridge ID priority for an MISTP instance when the switch is in MISTP or MISTP-PVST+ mode.

The bridge priority value is combined with the system ID extension (the ID of the MISTP instance) to create the bridge ID priority. You can set 16 possible bridge priority values: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, and 61440.

To configure the bridge ID priority for an MISTP instance, perform this task in privileged mode:

	Task	Command
Step 1	Configure the bridge ID priority for an MISTP instance.	**set spantree priority** *bridge_ID_priority* [**mistp-instance** *instance*]
Step 2	Verify the bridge ID priority.	**show spantree mistp-instance** *instance* [*mod/port*] **active**

This example shows how to configure the bridge ID priority for an MISTP instance:

```
Console> (enable) set spantree priority 8192 mistp-instance 1
Spantree 1 bridge ID priority set to 8193
(bridge priority: 8192 + sys ID extension: 1)
Console> (enable) show spantree mistp-instance 1
VLAN 1
Spanning tree mode          MISTP
Spanning tree type          ieee
Spanning tree enabled
VLAN mapped to MISTP Instance: 1

Bridge ID MAC ADDR          00-d0-00-4c-18-00
Bridge ID Priority          8193 (bridge priority: 8192, sys ID ext: 1)
Bridge Max Age 20 sec   Hello Time 2 sec   Forward Delay 15 sec

Port                     Vlan Port-State    Cost      Prio Portfast Channel_id
------------------------ ---- ------------ --------- ---- -------- ----------
 1/1                     1    not-connected     20000   32 disabled 0
 1/2                     1    not-connected     20000   32 disabled 0
 2/1                     1    not-connected   2000000   32 disabled 0
 2/2                     1    not-connected   2000000   32 disabled 0
 2/3                     1    forwarding       200000   32 disabled 0
```

Configuring the MISTP Port Cost

You can configure the port cost of switch ports. Ports with lower port costs are more likely to be chosen to forward frames. Assign lower numbers to ports attached to faster media (such as full duplex) and higher numbers to ports attached to slower media. The possible range is 1 to 65535. The default differs for different media. The path cost is typically 1000 divided by the LAN speed in megabits per second.

To configure the port cost for a port, perform this task in privileged mode:

	Task	Command
Step 1	Configure the MISTP port cost for a switch port.	**set spantree portcost** *mod/port cost*
Step 2	Verify the port cost setting.	**show spantree mistp-instance** *instance* [*mod/port*] **active**

This example shows how to configure the port cost on a MISTP instance and verify the configuration:

```
Console> (enable) set spantree portcost 2/12 22222222
Spantree port 2/12 path cost set to 22222222.
Console> (enable) show spantree mistp-instance active
Instance 1
Spanning tree mode          MISTP-PVST+
Spanning tree type          ieee
Spanning tree instance enabled

Designated Root             00-d0-00-4c-18-00
Designated Root Priority    32769 (root priority: 32768, sys ID ext: 1)
Designated Root Cost        0
Designated Root Port        none
VLANs mapped:               6
Root Max Age   20 sec   Hello Time 2 sec   Forward Delay 15 sec

Bridge ID MAC ADDR          00-d0-00-4c-18-00
Bridge ID Priority          32769 (bridge priority: 32768, sys ID ext: 1)
VLANs mapped:               6
Bridge Max Age 20 sec   Hello Time 2 sec   Forward Delay 15 sec

Port                     Inst Port-State    Cost      Prio Portfast Channel_id
------------------------ ---- ------------ --------- ---- -------- ----------
 2/12                    1    forwarding     22222222   40 disabled 0
Console> (enable)
```

Configuring the MISTP Port Priority

You can configure the port priority of ports. The port with the lowest priority value forwards frames for all VLANs. The possible port priority value is a multiple of 16 from 0 to 240. The default is 32. If all ports have the same priority value, the port with the lowest port number forwards frames.

To configure the port priority for a port, perform this task in privileged mode:

	Task	Command
Step 1	Configure the MISTP port priority for a port.	**set spantree portpri** *mod/port*
Step 2	Verify the port priority setting.	**show spantree mistp-instance** *instance* [*mod/port*] **active**

3330
RQS Nº 03/2005 - CN
CPMI - CORREIOS
0752
Fls:
3701
Doc:

This example shows how to configure the port priority and verify the configuration:

```
Console> (enable) set spantree portpri 2/12 40
Bridge port 2/12 port priority set to 40.
Console> (enable) show spantree mistp-instance 1
Instance 1
Spanning tree mode          MISTP-PVST+
Spanning tree type          ieee
Spanning tree instance enabled

Designated Root             00-d0-00-4c-18-00
Designated Root Priority    32769 (root priority: 32768, sys ID ext: 1)
Designated Root Cost        0
Designated Root Port        none
VLANs mapped:               6
Root Max Age   20 sec   Hello Time 2 sec   Forward Delay 15 sec

Bridge ID MAC ADDR          00-d0-00-4c-18-00
Bridge ID Priority          32769 (bridge priority: 32768, sys ID ext: 1)
VLANs mapped:               6
Bridge Max Age 20 sec   Hello Time 2 sec   Forward Delay 15 sec

Port                     Inst Port-State    Cost      Prio Portfast Channel_id
------------------------ ---- ------------ --------- ---- -------- ----------
 2/12                    1    forwarding     22222222   40 disabled 0
Console> (enable)
```

Configuring the MISTP Port Instance Cost

You can configure the port instance cost for an instance of MISTP or MISTP-PVST+. Ports with a lower instance cost are more likely to be chosen to forward frames. You should assign lower numbers to ports attached to faster media (such as full duplex) and higher numbers to ports attached to slower media. The default cost differs for different media. The possible value for port instance cost is 1–268435456.

To configure the port instance cost for a port, perform this task in privileged mode:

Task	Command
Configure the MISTP port instance cost on a port.	**set spantree portinstancecost** {*mod/port*} [**cost** *cost*] [*instances*]

This example shows how to configure the MISTP port instance cost on a port:

```
Console> (enable) set spantree portinstancecost 2/12 cost 110110 2
Port 2/12 instances 1,3-16 have path cost 22222222.
Port 2/12 instances 2 have path cost 110110.
Console> (enable)
```

Configuring the MISTP Port Instance Priority

You can set the port priority for an instance of MISTP. The port with the lowest priority value for a specific MISTP instance forwards frames for that instance. The possible port instance range is 0–63. The possible port priority value is a multiple of 16 from 0 to 240. If all ports have the same priority value for an MISTP instance, the port with the lowest port number forwards frames for that instance.

To configure the port instance priority on an MISTP instance, perform this task in privileged mode:

Task	Command
Configure the port instance priority on an MISTP instance.	**set spantree portinstancepri** {*mod/port*} *priority* [*instances*]

This example shows how to configure the port instance priority on an MISTP instance and verify the configuration:

```
Console> (enable) set spantree portinstancepri 2/12 10 2
Port 2/12 instances 2 using portpri 10.
Port 2/12 mistp-instance 1,3-16 using portpri 40.
Console> (enable)
```

Enabling an MISTP Instance

You can enable up to 16 MISTP instances. Each MISTP instance defines a unique spanning tree topology. MISTP instance 1, the default instance, is enabled by default; however, you must map a VLAN to it in order for it to be active. You can enable a single MISTP instance, a range of instances, or all instances at once using the **all** keyword.

Note The software does not display the status of an MISTP instance until it has a VLAN with an active port mapped to it.

To enable an MISTP instance, perform this task in privileged mode:

	Task	Command
Step 1	Enable an MISTP instance.	**set spantree enable mistp-instance** *instance* **[all]**
Step 2	Verify the instance is enabled.	**show spantree mistp-instance** [*instance*] **[active]** *mod/port*

Note Enter the **active** keyword to display active ports only.

This example shows how to enable an MISTP instance:

```
Console> (enable) set spantree enable mistp-instance 2
Spantree 2 enabled.

Console> (enable) show spantree mistp-instance 2
Instance 2
Spanning tree mode          MISTP
Spanning tree type          ieee
Spanning tree instance enabled
   .
   .
   .
```

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0753
Fls:
3701
Doc:

Mapping VLANs to an MISTP Instance

When you are using MISTP-PVST+ or MISTP on a switch, you must map at least one VLAN to an MISTP instance in order for MISTP-PVST+ or MISTP to be active. These sections describe how to configure MISTP instances:

- Determining MISTP Instances—VLAN Mapping Conflicts, page 8-37
- Unmapping VLANs from an MISTP Instance, page 8-37

Note See Chapter 11, "Configuring VLANs" for details on using and configuring VLANs.

- You can only map Ethernet VLANs to MISTP instances.
- At least one VLAN in the instance must have an active port in order for MISTP-PVST+ or MISTP to be active.
- You can map as many Ethernet VLANs as you wish to an MISTP instance.
- You cannot map a VLAN to more than one MISTP instance.

Note To use VLANs 1025–4094, you must enable MAC address reduction. See the "Creating Extended-Range VLANs" section on page 11-7 in Chapter 11, "Configuring VLANs" for details on using extended-range VLANs.

To map a VLAN to an MISTP instance, perform this task in privileged mode:

	Task	Command
Step 1	Map a VLAN to an MISTP instance.	**set vlan** *vlan* **mistp-instance** *instance*
Step 2	Verify the VLAN is mapped.	**show spantree mistp-instance** [*instance*] **[active]** *mod/port*

This example shows how to map a VLAN to MISTP instance 1 and verify the mapping:

```
Console> (enable) set vlan 6 mistp-instance 1
Vlan 6 configuration successful
Console> (enable) show spantree mist-instance 1
Instance 1
Spanning tree mode          MISTP-PVST+
Spanning tree type          ieee
Spanning tree instance enabled

Designated Root             00-d0-00-4c-18-00
Designated Root Priority    49153 (root priority: 49152, sys ID ext: 1)
Designated Root Cost        0
Designated Root Port        none
VLANs mapped:               6
Root Max Age   20 sec   Hello Time 2 sec   Forward Delay 15 sec

Bridge ID MAC ADDR          00-d0-00-4c-18-00
Bridge ID Priority          49153 (bridge priority: 49152, sys ID ext: 1)
VLANs mapped:               6
Bridge Max Age 20 sec   Hello Time 2 sec   Forward Delay 15 sec
Port                    Inst Port-State    Cost      Prio Portfast Channel_id
----------------------- ---- ------------- --------- ---- -------- ----------
 2/12                   1    forwarding     22222222   40 disabled 0
```

Determining MISTP Instances—VLAN Mapping Conflicts

A VLAN can only be mapped to one MISTP instance. If you attempt to map a VLAN to more than one instance, all of its ports are set to blocking mode. You can use the **show spantree conflicts** command to determine to which MISTP instances you have attempted to map the VLAN.

This command prints a list of the MISTP instances associated with the VLAN, the MAC addresses of the root switches that are sending the BPDUs containing the VLAN mapping information, and the timers associated with the mapping of a VLAN to an MISTP instance. When only one entry is printed or when all the entries are associated to the same instance, the VLAN is mapped to that instance. If two or more entries in the list are associated with different MISTP instances, the VLAN is in conflict.

To clear up the conflict, you must manually remove the incorrect mapping(s) from the root switch. The remaining entry on the list becomes the official mapping.

To determine VLAN mapping conflicts, perform this task in privileged mode:

Task	Command
Determine VLAN mapping conflicts.	**show spantree conflicts** *vlan*

This example shows there is an attempt to map VLAN 2 to MISTP instance 1 and to MISTP instance 3 on two different switches as seen from a third switch in the topology:

```
Console> (enable) show spantree conflicts 2
Inst MAC               Delay     Time left
---- ----------------- --------- ---------
1    00-30-a3-4a-0c-00 inactive        20
3    00-30-f1-e5-00-01 inactive        10
```

The Delay timer shows the time in seconds remaining before the VLAN joins the instance. The field displays *inactive* if the VLAN is already mapped to an instance (the timer has expired), or if the VLAN is in conflict between instances.

The Time Left timer shows the time in seconds left before the entry expires and is removed from the table. The timer is restarted every time an incoming BPDU confirms the mapping. Entries pertaining to the root switch show *inactive* on the root switch itself.

Unmapping VLANs from an MISTP Instance

The keyword **none** is used to unmap the specified VLANs from the MISTP instances to which they are currently mapped. When you unmap a VLAN from an MISTP instance, the resulting state of all the ports of the VLAN (if the VLAN exists) is *blocking*.

To unmap a VLAN or all VLANs from an MISTP instance, perform this task in privileged mode:

Task	Command
Unmap a VLAN from an MISTP instance.	**set vlan** *vlan* **mistp-instance none**

This example shows how to unmap a VLAN from an MISTP instance:

```
Console> (enable) set vlan 6 mistp-instance none
Vlan 6 configuration successful
```

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0754
Fls:
Doc: 370

Disabling MISTP-PVST+ or MISTP

When the switch is in MISTP mode, you disable spanning tree on an instance, not for the whole switch.

When you disable spanning tree on an MISTP instance, the instance still exists on the switch, all of the VLANs mapped to it have all of their ports forwarding, and the instance BPDUs are flooded.

To disable an MISTP instance, perform this task in privileged mode:

Task	Command
Disable an MISTP instance.	**set spantree disable mistp-instance** *instance* [**all**]

This example shows how to disable an MISTP instance:

```
Console> (enable) set spantree disable mistp-instance 2
MI-STP instance 2 disabled.
```

Configuring a Root Switch

These sections explain how to configure a root switch:

- Configuring a Primary Root Switch, page 8-38
- Configuring a Secondary Root Switch, page 8-39
- Configuring a Root Switch to Improve Convergence, page 8-40
- Using Root Guard—Preventing Switches from Becoming Root, page 8-41

Configuring a Primary Root Switch

You can set a root switch on a VLAN when the switch is in PVST+ mode or on an MISTP instance when the switch is in MISTP mode. You enter the **set spantree root** command to reduce the bridge priority (the value associated with the switch) from the default (32768) to a lower value, which allows the switch to become the root switch.

When you specify a switch as the primary root, the default bridge priority is modified so that it becomes the root for the specified VLANs. Set the bridge priority to 8192. If this setting does not result in the switch becoming a root, modify the bridge priority to be 1 less or the same as the bridge priority of the current root switch. Because different VLANs could potentially have different root switches, the bridge VLAN-priority chosen makes this switch the root for all the VLANs specified. If reducing the bridge priority as low as 1 still does not make the switch the root switch, the system displays a message.

Caution Enter the **set spantree root** command on backbone switches or distribution switches only, not on access switches.

To configure a switch as the primary root switch, perform this task in privileged mode:

Task	Command
Configure a switch as the primary root switch.	**set spantree root** [*vlans*] [**dia** *network_diameter*] [**hello** *hello_time*]

This example shows how to configure the primary root switch for VLANs 1–10:

```
Console> (enable) set spantree root 1-10 dia 4
VLANs 1-10 bridge priority set to 8192
VLANs 1-10 bridge max aging time set to 14 seconds.
VLANs 1-10 bridge hello time set to 2 seconds.
VLANs 1-10 bridge forward delay set to 9 seconds.
Switch is now the root switch for active VLANs 1-6.
Console> (enable)
```

To configure a switch as the primary root switch for an instance, perform this task in privileged mode:

Task	Command
Configure a switch as the primary root switch for an instance.	**set spantree root mistp-instance** *instance* [**dia** *network_diameter*] [**hello** *hello_time*]

This example shows how to configure the primary root switch for an instance:

```
Console> (enable) set spantree root mistp-instance 2-4 dia 4
Instances 2-4 bridge priority set to 8192
VLInstances 2-4 bridge max aging time set to 14 seconds.
Instances 2-4 bridge hello time set to 2 seconds.
Instances 2-4 bridge forward delay set to 9 seconds.
Switch is now the root switch for active Instances 1-6.
Console> (enable)
```

Configuring a Secondary Root Switch

You can set a secondary root switch on a VLAN when the switch is in PVST+ mode or on an MISTP instance when the switch is in MISTP mode.

The **set spantree root secondary** command reduces the bridge priority to 16,384, making it the probable candidate to become the root switch if the primary root switch fails. You can run this command on more than one switch to create multiple backup switches in case the primary root switch fails.

To configure a switch as the secondary root switch, perform this task in privileged mode:

Task	Command
Configure a switch as the secondary root switch.	**set spantree root** [**secondary**] *vlans* [**dia** *network_diameter*] [**hello** *hello_time*]

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0755
Fls:
Doc: 3701

This example shows how to configure the secondary root switch for VLANs 22 and 24:

```
Console> (enable) set spantree root secondary 22,24 dia 5 hello 1
VLANs 22,24 bridge priority set to 16384.
VLANs 22,24 bridge max aging time set to 10 seconds.
VLANs 22,24 bridge hello time set to 1 second.
VLANs 22,24 bridge forward delay set to 7 seconds.
Console> (enable)
```

To configure a switch as the secondary root switch for an instance, perform this task in privileged mode:

Task	Command
Configure a switch as the secondary root switch for an instance.	**set spantree root** [**secondary**] **mistp-instance** *instance* [**dia** *network_diameter*] [**hello** *hello_time*]

This example shows how to configure the secondary root switch for an instance:

```
Console> (enable) set spantree root secondary mistp-instance 2-4 dia 4
Instances 2-4 bridge priority set to 8192
VLInstances 2-4 bridge max aging time set to 14 seconds.
Instances 2-4 bridge hello time set to 2 seconds.
Instances 2-4 bridge forward delay set to 9 seconds.
Switch is now the root switch for active Instances 1-6.
Console> (enable)
```

Configuring a Root Switch to Improve Convergence

By lowering the values for the Hello Time, Forward Delay Timer, and Maximum Age Timer parameters on the root switch, you can reduce the convergence time. For information on configuring these timers, see the "Configuring Spanning Tree Timers" section on page 8-42.

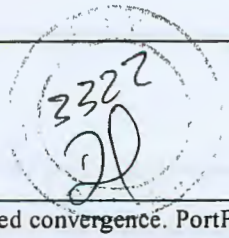
Note Reducing the timer parameters values is possible only if your network has LAN links of 10 Mbps or faster. In a network with links of 10 Mbps or faster, the network diameter can reach the maximum value of 7. With WAN connections, you cannot reduce the parameters.

When a link failure occurs in a bridged network, the network reconfiguration is not immediate. Reconfiguring the default parameters (specified by IEEE 802.1D) for the Hello Time, Forward Delay Timer, and Maximum Age Timer requires a 50-second delay. This reconfiguration time depends on the network diameter, which is the maximum number of bridges between any two end stations.

To speed up convergence, use nondefault parameter values permitted by the 802.1D standard. See Table 8-4 for the nondefault parameters for a reconvergence of 14 seconds.

Table 8-4 Nondefault Parameters

Parameter	Time
Network Diameter (dia)	2
Hello Time	2 seconds
Forward Delay Timer	4 seconds
Maximum Age Timer	6 seconds



Note You can set switch ports in PortFast mode for improved convergence. PortFast mode affects only the transition from disable (link down) to enable (link up) by moving the port immediately to the forwarding state. If a port in the PortFast mode begins blocking, it then goes through listening and learning before reaching the forwarding state. For information about PortFast, see the "Understanding How PortFast Works" section on page 9-2 in Chapter 9, "Configuring Spanning Tree PortFast, UplinkFast, BackboneFast, and Loop Guard."

To configure the spanning tree parameters to improve convergence, perform this task in privileged mode:

	Task	Command
Step 1	Configure the hello time for a VLAN or an MISTP instance.	**set spantree hello** *interval* [*vlan*] **mistp-instance** [*instances*]
Step 2	Verify the configuration.	**show spantree** [*vlan* | **mistp-instance** *instances*]
Step 3	Configure the forward delay time for a VLAN or an MISTP instance.	**set spantree fwddelay** *delay* [*vlan*] **mistp-instance** [*instances*]
Step 4	Verify the configuration.	**show spantree** [*mod/port*] **mistp-instance** [*instances*] [**active**]
Step 5	Configure the maximum aging time for a VLAN or an MISTP instance.	**set spantree maxage** *agingtime* [*vlans*] **mistp-instance** *instances*
Step 6	Verify the configuration.	**show spantree** [*mod/port*] **mistp-instance** [*instances*] [**active**]

This example shows how to configure the spanning tree hello time, Forward Delay Timer, and Maximum Age Timer to 2, 4, and 4 seconds:

```
Console> (enable) set spantree hello 2 100
Spantree 100 hello time set to 7 seconds.
Console> (enable)
Console> (enable) set spantree fwddelay 4 100
Spantree 100 forward delay set to 21 seconds.
Console> (enable)
Console> (enable) set spantree maxage 6 100
Spantree 100 max aging time set to 36 seconds.
Console> (enable)
Console> (enable) set spantree root 1-10 dia 4
VLANs 1-10 bridge priority set to 8192
VLANs 1-10 bridge max aging time set to 14 seconds.
VLANs 1-10 bridge hello time set to 2 seconds.
VLANs 1-10 bridge forward delay set to 9 seconds.
Switch is now the root switch for active VLANs 1-6.
Console> (enable)
```

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 0756
Doc: 3701

Using Root Guard—Preventing Switches from Becoming Root

You may want to prevent switches from becoming the root switch. The root guard feature forces a port to become a designated port so that no switch on the other end of the link can become a root switch.

When you enable root guard on a per-port basis, it is automatically applied to all of the active VLANs to which that port belongs. When you disable root guard, it is disabled for the specified port(s). If a port goes into the root-inconsistent state, it automatically goes into the listening state.

To prevent switches from becoming root, perform this task in privileged mode:

	Task	Command
Step 1	Enable root guard on a port.	**set spantree guard** {**root** | **none**} *mod/port*
Step 2	Verify that root guard is enabled.	**show spantree guard** {*mod/port* | *vlan*} {**mistp-instance** *instance* | *mod/port*}

Configuring Spanning Tree Timers

Spanning tree timers affect the spanning tree performance. You can configure the spanning tree timers for a VLAN in PVST+ or an MISTP instance in MISTP mode. If you do not specify a VLAN when the switch is in PVST+ mode, VLAN 1 is assumed, or if you do not specify an MISTP instance when the switch is in MISTP mode, MISTP instance 1 is assumed.

These sections describe how to configure spanning tree timers:

- Configuring the Hello Time, page 8-43
- Configuring the Forward Delay Time, page 8-43
- Configuring the Maximum Aging Time, page 8-44

Caution Exercise care when using these commands. For most situations, we recommend that you use the **set spantree root** and **set spantree root secondary** commands to modify the spanning tree performance parameters.

Table 8-5 describes the switch variables that affect spanning tree performance.

Table 8-5 Spanning Tree Timers

Variable	Description	Default
Hello Time	Determines how often the switch broadcasts its hello message to other switches.	2 seconds
Maximum Age Timer	Measures the age of the received protocol information recorded for a port and ensures that this information is discarded when its age limit exceeds the value of the maximum age parameter recorded by the switch. The timeout value is the maximum age parameter of the switches.	20 seconds
Forward Delay Timer	Monitors the time spent by a port in the learning and listening states. The timeout value is the forward delay parameter of the switches.	15 seconds

Configuring the Hello Time

Enter the **set spantree hello** command to change the hello time for a VLAN or for an MISTP instance. The possible range of *interval* is 1 to 10 seconds.

To configure the spanning tree bridge hello time for a VLAN or an MISTP instance, perform this task in privileged mode:

	Task	Command
Step 1	Configure the hello time for a VLAN or an MISTP instance.	**set spantree hello** *interval* [*vlan*] **mistp-instance** [*instances*]
Step 2	Verify the configuration.	**show spantree** [*vlan* | **mistp-instance** *instances*]

This example shows how to configure the spanning tree hello time for VLAN 100 to 7 seconds:

```
Console> (enable) set spantree hello 7 100
Spantree 100 hello time set to 7 seconds.
Console> (enable)
```

This example shows how to configure the spanning tree hello time for an instance to 3 seconds:

```
Console> (enable) set spantree hello 3 mistp-instance 1
Spantree 1 hello time set to 3 seconds.
Console> (enable)
```

Configuring the Forward Delay Time

Enter the **set spantree fwddelay** command to configure the spanning tree forward delay time for a VLAN. The possible range of *delay* is 4 to 30 seconds.

To configure the spanning tree forward delay time for a VLAN, perform this task in privileged mode:

	Task	Command
Step 1	Configure the forward delay time for a VLAN or an MISTP instance.	**set spantree fwddelay** *delay* [*vlan*] **mistp-instance** [*instances*]
Step 2	Verify the configuration.	**show spantree** [*mod/port*] **mistp-instance** [*instances*] **[active]**

This example shows how to configure the spanning tree forward delay time for VLAN 100 to 21 seconds:

```
Console> (enable) set spantree fwddelay 21 100
Spantree 100 forward delay set to 21 seconds.
Console> (enable)
```

This example shows how to set the bridge forward delay for an instance to 16 seconds:

```
Console> (enable) set spantree fwddelay 16 mistp-instance 1
Instance 1 forward delay set to 16 seconds.
Console> (enable)
```

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0757
Fls:
Doc: 3701

Configuring the Maximum Aging Time

Enter the **set spantree maxage** command to change the spanning tree maximum aging time for a VLAN or an instance. The possible range of *agingtime* is 6 to 40 seconds.

To configure the spanning tree maximum aging time for a VLAN or an instance, perform this task in privileged mode:

	Task	Command
Step 1	Configure the maximum aging time for a VLAN or an MISTP instance.	**set spantree maxage** *agingtime* [*vlans*] **mistp-instance** *instances*
Step 2	Verify the configuration.	**show spantree** [*mod/port*] **mistp-instance** [*instances*] [**active**]

This example shows how to configure the spanning tree maximum aging time for VLAN 100 to 36 seconds:

```
Console> (enable) set spantree maxage 36 100
Spantree 100 max aging time set to 36 seconds.
Console> (enable)
```

This example shows how to set the maximum aging time for an instance to 25 seconds:

```
Console> (enable) set spantree maxage 25 mistp-instance 1
Instance 1 max aging time set to 25 seconds.
Console> (enable)
```

Configuring Multiple Spanning Tree

These sections describe how to configure MST:

- Enabling Multiple Spanning Tree, page 8-44
- Mapping and Unmapping VLANs to an MST Instance, page 8-53

Enabling Multiple Spanning Tree

To enable and configure MST on the switch, perform these tasks in privileged mode:

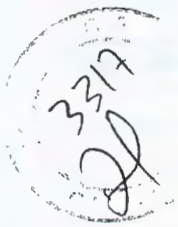
	Task	Command
Step 1	Begin in PVST+ mode.	**set spantree mode pvst+ [mistp | pvst+ | mistp-pvst+ | mst]**
Step 2	Display the STP ports.	**show spantree active**
Step 3	Configure the MST region.	**set spantree mst config {[name** *name*] **|** [**revision** *number*] [**commit | rollback | force**]}
Step 4	Verify your configuration.	**show spantree mst config**
Step 5	Map VLANs to the MST instance.	**set spantree mst** *instance* **vlan** *vlan*
Step 6	Commit the new region mapping.	**set spantree mst config commit**

	Task	Command
Step 7	Enable MST.	**set spantree mode mst** [**mistp** | **pvst+** | **mistp-pvst+** | **mst**]
Step 8	Verify your MST configuration.	**show spantree mst config**
Step 9	Verify your MST instance configuration.	**show spantree mst** *instance*
Step 10	Verify your MST module and port configuration.	**show spantree mst** *mod/port*

These examples show how to enable MST:

```
Console> (enable)
Console> (enable) set spantree mode pvst
Spantree mode set to PVST+.
Console> (enable) show spantree active
VLAN 1
Spanning tree mode          PVST+
Spanning tree type          ieee
Spanning tree enabled

Designated Root             00-50-3e-66-d0-00
Designated Root Priority    24576
Designated Root Cost        104
Designated Root Port        6/1
Root Max Age   20 sec   Hello Time 2  sec   Forward Delay 15 sec

Bridge ID MAC ADDR          00-10-7b-bb-2f-00
Bridge ID Priority          32768
Bridge Max Age 20 sec   Hello Time 2  sec   Forward Delay 15 sec

Port                     Vlan Port-State    Cost       Prio Portfast
Channel_id
------------------------ ---- ------------- --------- ---- ------------------
 6/1                     1    forwarding            4   32 disabled 0
 6/2                     1    blocking              4   32 disabled 0
Console> (enable)
Console> (enable) set spantree mst config name cisco revision 1
Edit Buffer modified. Use 'set spantree mst config commit' to apply the
changes.
Console> (enable) show spantree mst config
Current (NVRAM) MST Region Configuration:
Configuration Name:                                  Revision:0
Instance VLANs
-------- ------------------------------------------------------------------
IST      1-4094
  1      -
  2      -
  3      -
  4      -
  5      -
  6      -
  7      -
  8      -
  9      -
 10      -
 11      -
 12      -
 13      -
 14      -
 15      -
==========================================================================
```

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0758
Fls:
Doc: 3701



```
NEW MST Region Configuration (Not committed yet)
Configuration Name:cisco                                    Revision:1
Instance VLANs
-------- ----------------------------------------------------------------
IST      1-4094
  1      -
  2      -
  3      -
  4      -
  5      -
  6      -
  7      -
  8      -
  9      -
 10      -
 11      -
 12      -
 13      -
 14      -
 15      -
================================================================================
Edit buffer is locked by:Console (pid 142)
Console> (enable)
Console> (enable) set spantree mst 1 vlan 2-10
Edit Buffer modified. Use 'set spantree mst config commit' to apply the
changes.
Console> (enable) set spantree mst 1 vlan 2-20
Edit Buffer modified. Use 'set spantree mst config commit' to apply the
changes.
Console> (enable) set spantree mst 2 vlan 21-30
Edit Buffer modified. Use 'set spantree mst config commit' to apply the
changes.
Console> (enable) set spantree mst 3 vlan 31-40
Edit Buffer modified. Use 'set spantree mst config commit' to apply the
changes.
Console> (enable) set spantree mst 4 vlan 41-50
Edit Buffer modified. Use 'set spantree mst config commit' to apply the
changes.
Console> (enable)
Console> (enable) show spantree mst config
Current (NVRAM) MST Region Configuration:
Configuration Name:                                         Revision:0
Instance VLANs
-------- ----------------------------------------------------------------
IST      1-4094
  1      -
  2      -
  3      -
  4      -
  5      -
  6      -
  7      -
  8      -
  9      -
 10      -
 11      -
 12      -
 13      -
 14      -
 15      -
================================================================================
```

```
NEW MST Region Configuration (Not committed yet)
Configuration Name:cisco                                    Revision:1
Instance VLANs
-------- ----------------------------------------------------------------
IST      1,51-4094
  1      2-20
  2      21-30
  3      31-40
  4      41-50
  5      -
  6      -
  7      -
  8      -
  9      -
 10      -
 11      -
 12      -
 13      -
 14      -
 15      -
================================================================================
Edit buffer is locked by:Console (pid 142)
Console> (enable)
Console> (enable) set spantree mst config commit
Console> (enable)
Console> (enable) show spantree mst config
Current (NVRAM) MST Region Configuration:
Configuration Name:cisco                                    Revision:1
Instance VLANs
-------- ----------------------------------------------------------------
IST      1,51-4094
  1      2-20
  2      21-30
  3      31-40
  4      41-50
  5      -
  6      -
  7      -
  8      -
  9      -
 10      -
 11      -
 12      -
 13      -
 14      -
 15      -
================================================================================
Console> (enable)
Console> (enable) set spantree mode mst
PVST+ database cleaned up.
Spantree mode set to MST.
Console> (enable)
Console> (enable)
Console> (enable) show spantree mst 0
Spanning tree mode          MST
Instance                    0
VLANs Mapped:               1,51-4094

Designated Root             00-50-3e-66-d0-00
Designated Root Priority    24576  (root priority:24576, sys ID ext:0)

Designated Root Cost        20100
Designated Root Port        6/1
Root Max Age   20 sec   Hello Time 2  sec   Forward Delay 15 sec
```

3316
20

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0759
Fls:
Doc: 3701

```
IST Master ID MAC ADDR       00-10-7b-bb-2f-00
IST Master ID Priority       32768
IST Master Path Cost         0          Remaining Hops 20

Bridge ID MAC ADDR           00-10-7b-bb-2f-00
Bridge ID Priority           32768  (bridge priority:32768, sys ID ext:
0)
Bridge Max Age 20 sec   Hello Time 2  sec   Forward Delay 15 sec  Max
Hops 20

Port                     State         Role Cost     Prio Type
------------------------ ------------- ---- -------- -------------------------
 6/1                     forwarding    ROOT    20000   32 P2P,
Boundary(PVST)
 6/2                     blocking      ALTR    20000   32 P2P,
Boundary(PVST)
Console> (enable) show spantree mst 1
Spanning tree mode           MST
Instance                     1
VLANs Mapped:                2-20

Designated Root              00-10-7b-bb-2f-00
Designated Root Priority     32769  (root priority:32768, sys ID ext:1)

Designated Root Cost         0          Remaining Hops 20
Designated Root Port         1/0

Bridge ID MAC ADDR           00-10-7b-bb-2f-00
Bridge ID Priority           32769  (bridge priority:32768, sys ID ext:
1)

Port                     State         Role Cost     Prio Type
------------------------ ------------- ---- -------- -------------------------
 6/1                     forwarding    BDRY    20000   32 P2P,
Boundary(PVST)
 6/2                     blocking      BDRY    20000   32 P2P,
Boundary(PVST)
Console> (enable)
Console> (enable)
Console> (enable) show spantree mst 6/1
Edge Port:       No,  (Configured) Default
Link Type:      P2P,  (Configured) Auto
Port Guard:   Default
Boundary:     Yes (PVST)

Inst State         Role Cost      Prio VLANs
---- ------------- ---- --------- ---------------------------------------
   0 forwarding    ROOT     20000   32 1
   1 forwarding    BDRY     20000   32 2-20
   2 forwarding    BDRY     20000   32 21-30
   3 forwarding    BDRY     20000   32 31-40
   4 forwarding    BDRY     20000   32 41-50
Console> (enable)
Console> (enable) show spantree mst config
Current (NVRAM) MST Region Configuration:
Configuration Name:cisco                                Revision:1
```

```
Instance VLANs
-------- ---------------------------------------------------------------
IST      1,51-4094
  1      2-20
  2      21-30
  3      31-40
  4      41-50
  5      -
  6      -
  7      -
  8      -
  9      -
 10      -
 11      -
 12      -
 13      -
 14      -
 15      -
=======================================================================
Console> (enable)
```

Configuring the MST Bridge ID Priority

You can set the bridge ID priority for an MST instance when the switch is in MST mode.

The bridge priority value is combined with the system ID extension (the ID of the MST instance) to create the bridge ID priority. You can set 16 possible bridge priority values: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, and 61440.

To configure the bridge ID priority for an MST instance, perform this task in privileged mode:

	Task	Command
Step 1	Configure the bridge ID priority for an MST instance.	**set spantree priority** *bridge_priority* **mst** [*instance*]
Step 2	Verify the bridge ID priority.	**show spantree mst** [*instance* | *mod/port*]

The example shows how to configure the bridge ID priority for an MST instance:

```
Console> (enable) set spantree priority 8192 mst 3
MST Spantree 3 bridge priority set to 8192.
Console> (enable)
Console> (enable) show spantree mst 3
Spanning tree mode          MST
Instance                    3
VLANs Mapped:               31-40

Designated Root             00-10-7b-bb-2f-00
Designated Root Priority    8195  (root priority:8192, sys ID ext:3)
Designated Root Cost        0           Remaining Hops 20
Designated Root Port        1/0

Bridge ID MAC ADDR          00-10-7b-bb-2f-00
Bridge ID Priority          8195  (bridge priority:8192, sys ID ext:3)
```

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0760
Fls:
Doc 3701

```
Port                     State         Role Cost     Prio Type
------------------------ ------------- ---- -------- ------------------------
 6/1                     forwarding    BDRY    20000   32 P2P,
Boundary(PVST)
 6/2                     blocking      BDRY    20000   32 P2P,
Boundary(PVST)
```

Configuring the MST Port Cost

You can configure the port cost of switch ports. Ports with lower port costs are more likely to be chosen to forward frames. Assign lower numbers to ports attached to faster media (such as full duplex) and higher numbers to ports attached to slower media. The possible range is 1 to 65535. The default differs for different media. The path cost is typically 1000 divided by the LAN speed in megabits per second.

To configure the port cost for a port, perform this task in privileged mode:

	Task	Command
Step 1	Configure the MST port cost for a switch port.	**set spantree portcost** *mod/port cost* [**mst**]
Step 2	Verify the port cost setting.	**show spantree mst** [*instance* | *mod/port*]

This example shows how to configure the port cost on an MST instance and verify the configuration:

```
Console> (enable) set spantree portcost 6/1 10000 mst
Spantree port 6/1 path cost set to 10000.
Console> (enable)
Console> (enable) show spantree mst 6/1
Edge Port:       No,   (Configured) Default
Link Type:       P2P,  (Configured) Auto
Port Guard:   Default
Boundary:     Yes (PVST)

Inst State         Role Cost      Prio VLANs
---- ------------- ---- --------- ----------------------------------------
   0 forwarding    ROOT     10000   32 1
   1 forwarding    BDRY     10000   32 2-20
   2 forwarding    BDRY     10000   32 21-30
   3 forwarding    BDRY     10000   32 31-40
   4 forwarding    BDRY     10000   32 41-50
Console> (enable)
```

Configuring the MST Port Priority

You can configure the port priority of ports. The port with the lowest priority value forwards frames for all VLANs. The possible port priority value is a multiple of 16 from 0 to 240. The default is 32. If all ports have the same priority value, the port with the lowest port number forwards frames.

To configure the port priority for a port, perform this task in privileged mode:

	Task	Command
Step 1	Configure the MST port priority for a port.	**set spantree portpri** *mod/port priority* [**mst**]
Step 2	Verify the port priority setting.	**show spantree mst** [*instance* | *mod/port*]

This example shows how to configure the port priority and verify the configuration:

```
Console> (enable) set spantree portpri 6/1 30 mst
Bridge port  6/1 port priority set to 30.
Console> (enable)
Console> (enable) show spantree mst 6/1
Edge Port:        No,  (Configured) Default
Link Type:       P2P,  (Configured) Auto
Port Guard:    Default
Boundary:      Yes (PVST)

Inst State         Role Cost      Prio VLANs
---- ------------- ---- --------- ---------------------------------------
   0 forwarding    ROOT     10000   30 1
   1 forwarding    BDRY     10000   30 2-20
   2 forwarding    BDRY     10000   30 21-30
   3 forwarding    BDRY     10000   30 31-40
   4 forwarding    BDRY     10000   30 41-50
Console> (enable)
```

Configuring the MST Port Instance Cost

You can configure the port instance cost for an instance of MST. Ports with a lower instance cost are more likely to be chosen to forward frames. You should assign lower numbers to ports attached to faster media (such as full duplex) and higher numbers to ports attached to slower media. The default cost differs for different media. The possible value for port instance cost is 1–268435456.

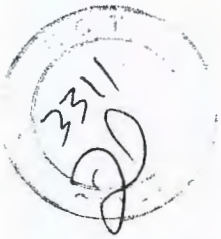
To configure the port instance cost for a port, perform this task in privileged mode:

	Task	Command
Step 1	Configure the MST port instance cost on a port.	**set spantree portinstancecost** *mod/port* [**cost** *cost*] **mst** [*instances*]
Step 2	Verify the path cost for the instances on a port.	**show spantree portinstancecost** *mod/port*

This example shows how to configure the MST port instance cost on a port:

```
Console> (enable) set spantree portinstancecost 6/1 cost 5000 mst 4
Port 6/1 MST Instances 0-3,5-15 have path cost 10000.
Port 6/1 MST Instances 4 have path cost 5000.
Console> (enable)
Console> (enable) show spantree mst 4
Spanning tree mode          MST
Instance                    4
VLANs Mapped:               41-50

Designated Root             00-10-7b-bb-2f-00
Designated Root Priority    32772  (root priority:32768, sys ID ext:4)

Designated Root Cost        0          Remaining Hops 20
Designated Root Port        1/0

Bridge ID MAC ADDR          00-10-7b-bb-2f-00
Bridge ID Priority          32772  (bridge priority:32768, sys ID ext:
4)
```

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 0761
Doc: 3701



```
Port                     State         Role Cost     Prio Type
------------------------ ------------- ---- -------- ------------------------
 6/1                     forwarding    BDRY     5000   30 P2P,
Boundary(PVST)
 6/2                     blocking      BDRY    20000   32 P2P,
Boundary(PVST)
Console> (enable)
```

Configuring the MST Port Instance Priority

You can set the port priority for an instance of MST. The port with the lowest priority value for a specific MST instance forwards frames for that instance. The possible port instance range is 0–240. If all ports have the same priority value for an MST instance, the port with the lowest port number forwards frames for that instance.

To configure the port instance priority on an MST instance, perform this task in privileged mode:

	Task	Command
Step 1	Configure the port instance priority on an MST instance.	**set spantree portinstancepri** *mod/port priority* **mst** [*instance*]
Step 2	Verify the port instance priority setting.	**show spantree mst** [*instance* | *mod/port*]

This example shows how to configure the port instance priority on an MST instance and verify the configuration:

```
Console> (enable) set spantree portinstancepri 6/1 16 mst 2
Port 6/1 MST Instances 2 using portpri 16.
Port 6/1 MST Instances 0-1,3-15 using portpri 30.
Console> (enable)
Console> (enable)
Console> (enable) show spantree mst 2
Spanning tree mode          MST
Instance                    2
VLANs Mapped:               21-30

Designated Root             00-10-7b-bb-2f-00
Designated Root Priority    32770  (root priority:32768, sys ID ext:2)

Designated Root Cost        0          Remaining Hops 20
Designated Root Port        1/0

Bridge ID MAC ADDR          00-10-7b-bb-2f-00
Bridge ID Priority          32770  (bridge priority:32768, sys ID ext:
2)

Port                     State         Role Cost     Prio Type
------------------------ ------------- ---- -------- ------------------------
 6/1                     forwarding    BDRY    10000   16 P2P,
Boundary(PVST)
 6/2                     blocking      BDRY    20000   32 P2P,
Boundary(PVST)
Console> (enable)
```

Mapping and Unmapping VLANs to an MST Instance

By default, all VLANS are mapped to IST (instance 0). For an MST instance (MSTI) 1 through 15 to be active, at least one VLAN must be mapped to that MSTI. IST will always be active whether VLANs are mapped to IST or not. MST has separate regions, which prevents VLAN mapping conflicts. Follow these guidelines for mapping and unmapping VLANS to an MST instance:

Note See Chapter 11, "Configuring VLANs" for details on using and configuring VLANs.

- You can only map Ethernet VLANs to MST instances.
- At least one VLAN in the instance must have an active port in order for MST to be active.
- You can map as many Ethernet VLANs as you wish to an MST instance.
- You cannot map a VLAN to more than one MST instance.
- The Hello Time, Maximum Age timer, and Forward Delay timer set for mode and all spanning trees are used globally by MST.

Note To use VLANs 1025–4094, you must enable MAC address reduction. See the "Creating Extended-Range VLANs" section on page 11-7 in Chapter 11, "Configuring VLANs" for details on using extended-range VLANs.

To map a VLAN to an MST instance, perform this task in privileged mode:

	Task	Command
Step 1	Map a VLAN to an MST instance.	**set spantree mst** *instance* **vlan** *vlan*
Step 2	Make the new region mapping effective.	**set spantree mst config commit**
Step 3	Verify the VLAN is mapped.	**show spantree mst** [*instance*] **[active]** *mod/port*

This example shows how to map a VLAN to MST instance 1 and verify the mapping:

```
Console> (enable) show spantree mst config
Current (NVRAM) MST Region Configuration:
Configuration Name:cisco                                    Revision:1
Instance VLANs
-------- ---------------------------------------------------------------
IST      1,51-4094
  1      2-20
  2      21-30
  3      31-40
  4      41-50
  5      -
  6      -
  7      -
  8      -
  9      -
 10      -
 11      -
 12      -
 13      -
 14      -
 15      -
```

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0762
Fls:
Doc: 3701

```
Console> (enable) set spantree mst 14 vlan 900-999
Edit Buffer modified. Use 'set spantree mst config commit' to apply the
changes.
Console> (enable) show spantree mst config
Current (NVRAM) MST Region Configuration:
Configuration Name:cisco                                    Revision:1
Instance VLANs
-------- ---------------------------------------------------------------
IST      1,51-4094
  1      2-20
  2      21-30
  3      31-40
  4      41-50
  5      -
  6      -
  7      -
  8      -
  9      -
 10      -
 11      -
 12      -
 13      -
 14      -
 15      -
================================================================================
NEW MST Region Configuration (Not committed yet)
Configuration Name:cisco                                    Revision:2
Instance VLANs
-------- ---------------------------------------------------------------
IST      1,51-899,1000-4094
  1      2-20
  2      21-30
  3      31-40
  4      41-50
  5      -
  6      -
  7      -
  8      -
  9      -
 10      -
 11      -
 12      -
 13      -
 14      900-999
 15      -
================================================================================
Edit buffer is locked by:Console (pid 142)
Console> (enable)
Console> (enable) clear spantree mst 14 vlan 900-998
Edit Buffer modified. Use 'set spantree mst config commit' to apply the
changes.
Console> (enable)
Console> (enable) show spantree mst config
Current (NVRAM) MST Region Configuration:
Configuration Name:cisco                                    Revision:1
Instance VLANs
-------- ---------------------------------------------------------------
IST      1,51-4094
  1      2-20
  2      21-30
  3      31-40
  4      41-50
  5      -
  6      -
```

```
  7       -
  8       -
  9       -
 10       -
 11       -
 12       -
 13       -
 14       -
 15       -
================================================================================
NEW MST Region Configuration (Not committed yet)
Configuration Name:cisco                                  Revision:2
Instance VLANs
-------- ----------------------------------------------------------------
IST      1,51-998,1000-4094
  1      2-20
  2      21-30
  3      31-40
  4      41-50
  5      -
  6      -
  7      -
  8      -
  9      -
 10      -
 11      -
 12      -
 13      -
 14      999
 15      -
================================================================================
Edit buffer is locked by:Console (pid 142)
Console> (enable)
Console> (enable) set spantree mst config commit
Console> (enable)
Console> (enable) show spantree mst config
Current (NVRAM) MST Region Configuration:
Configuration Name:cisco                                  Revision:2
Instance VLANs
-------- ----------------------------------------------------------------
IST      1,51-998,1000-4094
  1      2-20
  2      21-30
  3      31-40
  4      41-50
  5      -
  6      -
  7      -
  8      -
  9      -
 10      -
 11      -
 12      -
 13      -
 14      999
 15      -
================================================================================
Console> (enable)
```

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0763
Fls:
Doc:

```
Console> (enable) show spantree mst 3
Spanning tree mode          MST
Instance                    3
VLANs Mapped:               31-40

Designated Root             00-10-7b-bb-2f-00
Designated Root Priority    8195  (root priority:8192, sys ID ext:3)
Designated Root Cost        0          Remaining Hops 20
Designated Root Port        1/0

Bridge ID MAC ADDR          00-10-7b-bb-2f-00
Bridge ID Priority          8195  (bridge priority:8192, sys ID ext:3)

Port                    State         Role Cost     Prio Type
----------------------- ------------- ---- -------- ------------------------
 6/1                    forwarding    BDRY    10000   30 P2P,
Boundary(PVST)
 6/2                    blocking      BDRY    20000   32 P2P,
Boundary(PVST)
Console> (enable)
```

Configuring BPDU Skewing

Commands that support the spanning tree BPDU skewing feature perform these functions:

- Allow you to enable or disable BPDU skewing. The default is disabled.
- Modify the **show spantree summary** output to show if the skew detection is enabled and for which VLANs or PVST+ or MISTP instances the skew was detected.
- Provide a display of the VLAN or PVST+ or MISTP instance and the port affected by the skew including this information:
  - The last skew duration (in absolute time)
  - The worst skew duration (in absolute time)
  - The date and time of the worst duration

To change how spanning tree performs BPDU skewing statistics gathering, enter the **set spantree bpdu-skewing** command. The **bpdu-skewing** command is disabled by default.

To configure the BPDU skewing statistics gathering for a VLAN, perform this task in privileged mode:

	Task	Command
Step 1	Configure BPDU skewing.	**set spantree bpdu-skewing [enable | disable]**
Step 2	Verify the configuration.	**show spantree bpdu-skewing** *vlan* [*mod/port*] **show spantree bpdu-skewing mistp-instance** [*instance*] [*mod/port*]

This example shows how to configure BPDU skewing and view the skewing statistics:

```
Console> (enable) set spantree bpdu-skewing
Usage:set spantree bpdu-skewing <enable|disable>
Console> (enable) set spantree bpdu-skewing enable
Spantree bpdu-skewing enabled on this switch.
Console> (enable)
```

```
Console> (enable) show spantree bpdu-skewing 1
Bpdu skewing statistics for vlan 1
Port     Last Skew ms    Worst Skew ms      Worst Skew Time
------   -------------   -------------   -------------------------
8/2              5869          108370   Tue Nov 21 2000, 06:25:59
8/4              4050          113198   Tue Nov 21 2000, 06:26:04
8/6            113363          113363   Tue Nov 21 2000, 06:26:05
8/8              4111          113441   Tue Nov 21 2000, 06:26:05
8/10           113522          113522   Tue Nov 21 2000, 06:26:05
8/12             4111          113600   Tue Nov 21 2000, 06:26:05
8/14           113678          113678   Tue Nov 21 2000, 06:26:05
8/16             4111          113755   Tue Nov 21 2000, 06:26:05
8/18           113833          113833   Tue Nov 21 2000, 06:26:05
8/20             4111          113913   Tue Nov 21 2000, 06:26:05
8/22           113917          113917   Tue Nov 21 2000, 06:26:05
8/24             4110          113922   Tue Nov 21 2000, 06:26:05
8/26           113926          113926   Tue Nov 21 2000, 06:26:05
8/28             4111          113931   Tue Nov 21 2000, 06:26:05
Console> (enable)
```

This example shows how to configure BPDU skewing for VLAN 1 on module 8, port 2 and view the skewing statistics:

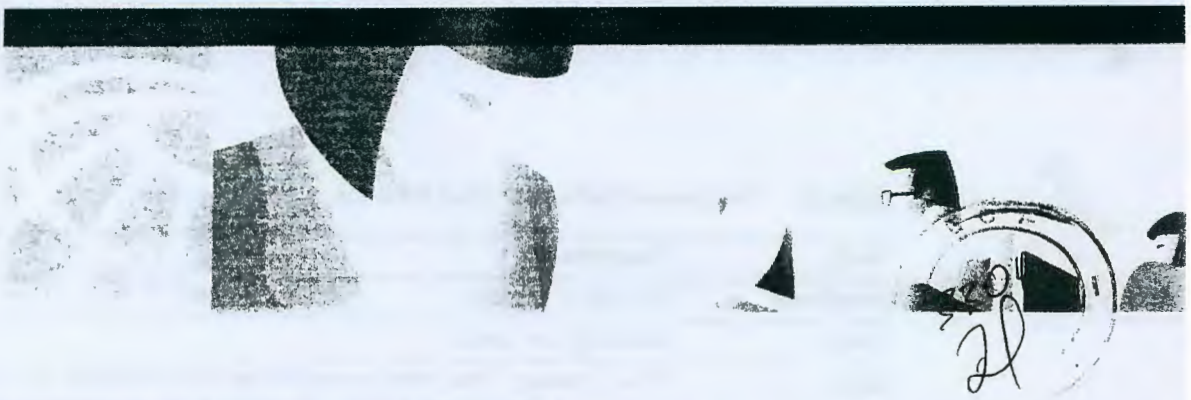
```
Console> (enable) show spantree bpdu-skewing 1 8/4
Bpdu skewing statistics for vlan 1
Port     Last Skew ms    Worst Skew ms      Worst Skew Time
------   -------------   -------------   -------------------------
8/4              5869          108370   Tue Nov 21 2000, 06:25:59
```

You will receive a similar output when MISTP is running.

The **show spantree summary** command displays if BPDU skew detection is enabled and also lists the VLANs or instances affected in the skew. This example shows the output when using the **show spantree summary** command:

```
Console> (enable) show spantree summary
Root switch for vlans: 1
BPDU skewing detection enabled for the bridge
BPDU skewed for vlans: 1
Portfast bpdu-guard disabled for bridge.
Portfast bpdu-filter disabled for bridge.
Uplinkfast disabled for bridge.
Backbonefast disabled for bridge.

Summary of connected spanning tree ports by vlan

VLAN  Blocking Listening Learning Forwarding STP Active
----- -------- --------- -------- ---------- ----------
    1        6         4        2          0         12

      Blocking Listening Learning Forwarding STP Active
----- -------- --------- -------- ---------- ----------
Total       6         4        2          0         12
Console> (enable)
```

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0764
Fls:
Doc: 3701



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.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0765
Fls:
3701
Doc:

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.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0766
Fls:
Doc: 3701

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.

FCC 05/2005 - CN
CPMI - CORREIOS
0767
Fls:
3701
Doc:

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 the 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.

3298

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

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0768
Fls:
Doc: 3701

- 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.

ECT Nº 03/2005 - N
CPMI - CORREIOS
0769
Fls:
Doc: 3701

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.

RQS N° 03/2005 - CN
CPMI - CORREIOS
0770
Doc: 3701

- 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... eeee
```

```
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:
!!!
```

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.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0772
Fls:
Doc: 3701

```
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
!!!
```

```
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...
```

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0773
Fls:
Doc 3701

```
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... eeee
```

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.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0774
Fls:
3701
Doc:

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.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0775
Fls:
Doc: 3701

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 IOS 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.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0776
Fls:
3701
Doc:

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... eeee
```

```
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.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0777
Fls:
Doc: 3701

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
```

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 0778
Doc: 3701

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.

RQS Nº 03/2005 - CN - CPMI - CORREIOS
0779
Fls:
Doc: 3701

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
```

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0780
Fls:
Doc: 3701

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
.
```

ROS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 0781
Doc: 3701

```
.
.
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.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 0782
Doc: 3701

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.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0783
Fls:
3701
Doc:

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.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0784
Fls:
Doc: 3701

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-1.a

tftp://dirt/hampton/c2500-j-1.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.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0785
Fls:
Doc: 3701

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.

ROS Nº 03/2005 - CN
CPMI - CORREIOS
0786
Fls:
3701
Doc:
FR-217

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
```

3259

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.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0787
Fls:
Doc:

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:
```

3257

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.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0788
Fls:
3701
Doc:

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 does 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.

ROS Nº 03/2005 - CN
CPMI - CORREIOS
0789
Fls:
Doc: 3701
FR-223

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.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0790
Fls: 3701
Doc:

Ap BQ

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 0791
Doc: 3791

CHAPTER 5

Configuring Ethernet VLAN Trunks

This chapter describes how to configure Ethernet VLAN trunks on the Catalyst 6500 series switches.

Note For complete information on configuring VLANs, see Chapter 11, "Configuring VLANs."

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:

- Understanding How VLAN Trunks Work, page 5-1
- Default Trunk Configuration, page 5-5
- Configuring a Trunk Link, page 5-5
- Example VLAN Trunk Configurations, page 5-9
- Disabling VLAN 1 on Trunks, page 5-23

Understanding How VLAN Trunks Work

These sections describe how VLAN trunks work on the Catalyst 6500 series switches:

- Trunking Overview, page 5-1
- Trunking Modes and Encapsulation Type, page 5-2
- 802.1Q Trunk Configuration Guidelines and Restrictions, page 5-4

Trunking Overview

A trunk is a point-to-point link between one or more Ethernet switch ports and another networking device such as a router or a switch. Trunks carry the traffic of multiple VLANs over a single link and allow you to extend VLANs across an entire network.

Two trunking encapsulations are available on all Ethernet ports:

- Inter-Switch Link (ISL)—ISL is a Cisco-proprietary trunking encapsulation
- IEEE 802.1Q—802.1Q is an industry-standard trunking encapsulation

RGSTN 03/2005 - CN
CPMI - CORREIOS
0792
Fls:
Doc: 3701

You can configure a trunk on a single Ethernet port or on an EtherChannel bundle. For more information about EtherChannel, see Chapter 6, "Configuring EtherChannel."

Ethernet trunk ports support five different trunking modes (see Table 5-1). In addition, you can specify whether the trunk will use ISL encapsulation, 802.1Q encapsulation, or whether the encapsulation type will be autonegotiated.

For trunking to be autonegotiated, the ports must be in the same VLAN Trunking Protocol (VTP) domain. However, you can use the **on** or **nonegotiate** mode to force a port to become a trunk, even if it is in a different domain. For more information on VTP domains, see Chapter 10, "Configuring VTP."

Trunk negotiation is managed by the Dynamic Trunking Protocol (DTP). DTP supports autonegotiation of both ISL and 802.1Q trunks.

Trunking Modes and Encapsulation Type

Note The 10-Gigabit Ethernet Switching Module does not support ISL encapsulation.

Table 5-1 lists the trunking modes used with the **set trunk** command and describes how they function on Fast Ethernet, Gigabit Ethernet, and 10-Gigabit Ethernet ports.

Table 5-1 Ethernet Trunking Modes

Mode	Function
on	Puts the port into permanent trunking mode and negotiates to convert the link into a trunk link. The port becomes a trunk port even if the neighboring port does not agree to the change.
off	Puts the port into permanent nontrunking mode and negotiates to convert the link into a nontrunk link. The port becomes a nontrunk port even if the neighboring port does not agree to the change.
desirable	Makes the port actively attempt to convert the link to a trunk link. The port becomes a trunk port if the neighboring port is set to **on**, **desirable**, or **auto** mode.
auto	Makes the port willing to convert the link to a trunk link. The port becomes a trunk port if the neighboring port is set to **on** or **desirable** mode. This is the default mode for all Ethernet ports.
nonegotiate	Puts the port into permanent trunking mode but prevents the port from generating DTP frames. You must configure the neighboring port manually as a trunk port to establish a trunk link.

Table 5-2 lists the encapsulation types used with the **set trunk** command and describes how they function on Ethernet ports. You can use the **show port capabilities** command to determine which encapsulation types a particular port supports.

Table 5-2 Ethernet Trunk Encapsulation Types

Encapsulation	Function
isl	Specifies ISL encapsulation on the trunk link.
dot1q	Specifies 802.1Q encapsulation on the trunk link.
negotiate	Specifies that the port negotiate with the neighboring port to become an ISL (preferred) or 802.1Q trunk, depending on the configuration and capabilities of the neighboring port.

The trunking mode, the trunk encapsulation type, and the hardware capabilities of the two connected ports determine whether a trunk link comes up and the type of trunk the link becomes. Table 5-3 shows the result of the possible trunking configurations.

Table 5-3 Results of Possible Fast Ethernet, Gigabit Ethernet, and 10-Gigabit Ethernet Trunk Configurations

Neighbor Port Trunk Mode and Trunk Encapsulation	Local Port Trunk Mode and Trunk Encapsulation								
	off isl or dot1q	**on isl**	**desirable isl**	**auto isl**	**on dot1q**	**desirable dot1q**	**auto dot1q**	**desirable negotiate**	**auto negotiate**
off isl or dot1q	Local: Nontrunk Neighbor: Nontrunk	Local: ISL trunk Neighbor: Nontrunk	Local: Nontrunk Neighbor: Nontrunk	Local: Nontrunk Neighbor: Nontrunk	Local: 1Q trunk Neighbor: Nontrunk	Local: Nontrunk Neighbor: Nontrunk	Local: Nontrunk Neighbor: Nontrunk	Local: Nontrunk Neighbor: Nontrunk	Local: Nontrunk Neighbor: Nontrunk
on isl	Local: Nontrunk Neighbor: ISL trunk	Local: ISL trunk Neighbor: ISL trunk	Local: ISL trunk Neighbor: ISL trunk	Local: ISL trunk Neighbor: ISL trunk	Local: 1Q trunk[1] Neighbor: ISL trunk[1]	Local: Nontrunk Neighbor: ISL trunk	Local: Nontrunk Neighbor: ISL trunk	Local: ISL trunk Neighbor: ISL trunk	Local: ISL trunk Neighbor: ISL trunk
desirable isl	Local: Nontrunk Neighbor: Nontrunk	Local: ISL trunk Neighbor: ISL trunk	Local: ISL trunk Neighbor: ISL trunk	Local: ISL trunk Neighbor: ISL trunk	Local: 1Q trunk Neighbor: Nontrunk	Local: Nontrunk Neighbor: Nontrunk	Local: Nontrunk Neighbor: Nontrunk	Local: ISL trunk Neighbor: ISL trunk	Local: ISL trunk Neighbor: ISL trunk
auto isl	Local: Nontrunk Neighbor: Nontrunk	Local: ISL trunk Neighbor: ISL trunk	Local: ISL trunk Neighbor: ISL trunk	Local: Nontrunk Neighbor: Nontrunk	Local: 1Q trunk Neighbor: Nontrunk	Local: Nontrunk Neighbor: Nontrunk	Local: Nontrunk Neighbor: Nontrunk	Local: ISL trunk Neighbor: ISL trunk	Local: Nontrunk Neighbor: Nontrunk
on dot1q	Local: Nontrunk Neighbor: 1Q trunk	Local: ISL trunk[1] Neighbor: 1Q trunk[1]	Local: Nontrunk Neighbor: 1Q trunk	Local: Nontrunk Neighbor: 1Q trunk	Local: 1Q trunk Neighbor: 1Q trunk	Local: 1Q trunk Neighbor: 1Q trunk	Local: 1Q trunk Neighbor: 1Q trunk	Local: 1Q trunk Neighbor: 1Q trunk	Local: 1Q trunk Neighbor: 1Q trunk
desirable dot1q	Local: Nontrunk Neighbor: Nontrunk	Local: ISL trunk Neighbor: Nontrunk	Local: Nontrunk Neighbor: Nontrunk	Local: Nontrunk Neighbor: Nontrunk	Local: 1Q trunk Neighbor: 1Q trunk	Local: 1Q trunk Neighbor: 1Q trunk	Local: 1Q trunk Neighbor: 1Q trunk	Local: 1Q trunk Neighbor: 1Q trunk	Local: 1Q trunk Neighbor: 1Q trunk
auto dot1q	Local: Nontrunk Neighbor: Nontrunk	Local: ISL trunk Neighbor: Nontrunk	Local: Nontrunk Neighbor: Nontrunk	Local: Nontrunk Neighbor: Nontrunk	Local: 1Q trunk Neighbor: 1Q trunk	Local: 1Q trunk Neighbor: 1Q trunk	Local: Nontrunk Neighbor: Nontrunk	Local: 1Q trunk Neighbor: 1Q trunk	Local: Nontrunk Neighbor: Nontrunk

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 3793
Doc.

Table 5-3 Results of Possible Fast Ethernet, Gigabit Ethernet, and 10-Gigabit Ethernet Trunk Configurations (continued)

Neighbor Port Trunk Mode and Trunk Encapsulation	Local Port Trunk Mode and Trunk Encapsulation								
	off isl or dot1q	on isl	desirable isl	auto isl	on dot1q	desirable dot1q	auto dot1q	desirable negotiate	auto negotiate
desirable negotiate	Local: Nontrunk Neighbor: Nontrunk	Local: ISL trunk Neighbor: ISL trunk	Local: ISL trunk Neighbor: ISL trunk	Local: ISL trunk Neighbor: ISL trunk	Local: 1Q trunk Neighbor: 1Q trunk	Local: 1Q trunk Neighbor: 1Q trunk	Local: 1Q trunk Neighbor: 1Q trunk	Local: ISL trunk Neighbor: ISL trunk	Local: ISL trunk Neighbor: ISL trunk
auto negotiate	Local: Nontrunk Neighbor: Nontrunk	Local: ISL trunk Neighbor: ISL trunk	Local: ISL trunk Neighbor: ISL trunk	Local: Nontrunk Neighbor: Nontrunk	Local: 1Q trunk Neighbor: 1Q trunk	Local: 1Q trunk Neighbor: 1Q trunk	Local: Nontrunk Neighbor: Nontrunk	Local: ISL trunk Neighbor: ISL trunk	Local: Nontrunk Neighbor: Nontrunk

1. Using this configuration can result in spanning tree loops and is not recommended.

Note DTP is a point-to-point protocol. However, some internetworking devices might forward DTP frames improperly. To avoid this problem, ensure that trunking is turned **off** on ports connected to non-switch devices if you do not intend to trunk across those links. When manually enabling trunking on a link to a Cisco router, use the **nonegotiate** keyword to cause the port to become a trunk but not generate DTP frames.

802.1Q Trunk Configuration Guidelines and Restrictions

The following configuration guidelines and restrictions apply when using 802.1Q trunks and impose some limitations on the trunking strategy for a network:

- When connecting Cisco switches through an 802.1Q trunk, make sure the native VLAN for an 802.1Q trunk is the same on both ends of the trunk link. If the native VLAN on one end of the trunk is different from the native VLAN on the other end, spanning tree loops might result.
- Disabling spanning tree on the native VLAN of an 802.1Q trunk without disabling spanning tree on every VLAN in the network can cause spanning tree loops. We recommend that you leave spanning tree enabled on the native VLAN of an 802.1Q trunk. If this is not possible, disable spanning tree on every VLAN in the network. Make sure your network is free of physical loops before disabling spanning tree.
- When you connect two Cisco switches through 802.1Q trunks, the switches exchange spanning tree BPDUs on each VLAN allowed on the trunks. The BPDUs on the native VLAN of the trunk are sent untagged to the reserved IEEE 802.1D spanning tree multicast MAC address (01-80-C2-00-00-00). The BPDUs on all other VLANs on the trunk are sent tagged to the reserved Cisco Shared Spanning Tree (SSTP) multicast MAC address (01-00-0c-cc-cc-cd).
- Non-Cisco 802.1Q switches maintain only a single instance of spanning tree (the Mono Spanning Tree, or MST) that defines the spanning-tree topology for all VLANs. When you connect a Cisco switch to a non-Cisco switch through an 802.1Q trunk, the MST of the non-Cisco switch and the native VLAN spanning-tree of the Cisco switch combine to form a single spanning-tree topology known as the Common Spanning Tree (CST).

When you connect a Cisco switch to a non-Cisco switch the CST is always on VLAN 1. The Cisco switch sends an untagged IEEE BDPU (01-80-C2-00-00-00) on VLAN 1 for the CST and on the native VLAN the Cisco switch sends an untagged Cisco BPDU (01-00-0C-CC-CC-CC) which the non-Cisco switch forwards but does not act on (the IEEE BPDU is not forwarded on the native VLAN).

- Because Cisco switches transmit BPDUs to the SSTP multicast MAC address on VLANs other than the native VLAN of the trunk, non-Cisco switches do not recognize these frames as BPDUs and flood them on all ports in the corresponding VLAN. Other Cisco switches connected to the non-Cisco 802.1Q cloud receive these flooded BPDUs. This allows Cisco switches to maintain a per-VLAN spanning tree topology across a cloud of non-Cisco 802.1Q switches. The non-Cisco 802.1Q cloud separating the Cisco switches is treated as a single broadcast segment between all switches connected to the non-Cisco 802.1Q cloud through 802.1Q trunks.
- Make certain that the native VLAN is the same on ALL of the 802.1Q trunks connecting the Cisco switches to the non-Cisco 802.1Q cloud.
- If you are connecting multiple Cisco switches to a non-Cisco 802.1Q cloud, all of the connections MUST be through 802.1Q trunks. You CANNOT connect Cisco switches to a non-Cisco 802.1Q cloud through ISL trunks or through access ports. Doing so will cause the switch to place the ISL trunk port or access port into the spanning tree "port inconsistent" state and no traffic will pass through the port.

Default Trunk Configuration

Table 5-4 shows the default Ethernet trunk configuration.

Table 5-4 Default Ethernet Trunk Configuration

Feature	Default Configuration
Trunk mode	**auto**
Trunk encapsulation	**negotiate**
Allowed VLAN range	VLANs 1–1005, 1025-4094

Configuring a Trunk Link

These sections describe how to configure a trunk link on Ethernet ports and how to define the allowed VLAN range on a trunk:

- Configuring an ISL Trunk, page 5-6
- Configuring an 802.1Q Trunk, page 5-7
- Configuring an ISL/802.1Q Negotiating Trunk Port, page 5-7
- Defining the Allowed VLANs on a Trunk, page 5-8
- Disabling a Trunk Port, page 5-9

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0794
Fls:
3701
Doc:

Configuring an ISL Trunk

To configure an ISL trunk, perform this task in privileged mode:

	Task	Command
Step 1	Configure an ISL trunk.	**set trunk** *mod/port* [**on** | **desirable** | **auto** | **nonegotiate**] **isl**
Step 2	Verify the trunking configuration.	**show trunk** [*mod/port*]

This example shows how to configure a port as a trunk and how to verify the trunk configuration. This example assumes that the neighboring port is in **auto** mode:

```
Console> (enable) set trunk 1/1 on
Port(s) 1/1 trunk mode set to on.
Console> (enable) 06/16/1998,22:16:39:DTP-5:Port 1/1 has become isl trunk
06/16/1998,22:16:40:PAGP-5:Port 1/1 left bridge port 1/1.
06/16/1998,22:16:40:PAGP-5:Port 1/1 joined bridge port 1/1.
Console> (enable) show trunk
Port      Mode         Encapsulation  Status        Native vlan
--------  -----------  -------------  ------------  -----------
 1/1      on           isl            trunking      1
Port      Vlans allowed on trunk
--------  ---------------------------------------------------------------------
 1/1      1-1005, 1025-4094

Port      Vlans allowed and active in management domain
--------  ---------------------------------------------------------------------
 1/1      1,521-524
Port      Vlans in spanning tree forwarding state and not pruned
--------  ---------------------------------------------------------------------
 1/1
Console> (enable)
```

This example shows how to place a port in **desirable** mode and how to verify the trunk configuration. This example assumes that the neighboring port is in **auto** mode:

```
Console> (enable) set trunk 1/2 desirable
Port(s) 1/2 trunk mode set to desirable.
Console> (enable) 06/16/1998,22:20:16:DTP-5:Port 1/2 has become isl trunk
06/16/1998,22:20:16:PAGP-5:Port 1/2 left bridge port 1/2.
06/16/1998,22:20:16:PAGP-5:Port 1/2 joined bridge port 1/2.
Console> (enable) show trunk 1/2
Port      Mode         Encapsulation  Status        Native vlan
--------  -----------  -------------  ------------  -----------
 1/2      desirable    isl            trunking      1
Port      Vlans allowed on trunk
--------  ---------------------------------------------------------------------
 1/2      1-1005, 1025-4094
Port      Vlans allowed and active in management domain
--------  ---------------------------------------------------------------------
 1/2      1,521-524
Port      Vlans in spanning tree forwarding state and not pruned
--------  ---------------------------------------------------------------------
 1/2
Console> (enable)
```

Configuring an 802.1Q Trunk

To configure an 802.1Q trunk, perform this task in privileged mode:

	Task	Command
Step 1	Configure an 802.1Q trunk.	**set trunk** *mod/port* [**on** | **desirable** | **auto** | **nonegotiate**] **dot1q**
Step 2	Verify the trunking configuration.	**show trunk** [*mod/port*]

This example shows how to configure an 802.1Q trunk and how to verify the trunk configuration:

```
Console> (enable) set trunk 2/9 desirable dot1q
Port(s) 2/9 trunk mode set to desirable.
Port(s) 2/9 trunk type set to dot1q.
Console> (enable) 07/02/1998,18:22:25:DTP-5:Port 2/9 has become dot1q trunk

Console> (enable) show trunk
Port      Mode         Encapsulation  Status        Native vlan
--------  -----------  -------------  ------------  -----------
 2/9      desirable    dot1q          trunking      1

Port      Vlans allowed on trunk
--------  ---------------------------------------------------------------------
 2/9      1-1005, 1025-4094

Port      Vlans allowed and active in management domain
--------  ---------------------------------------------------------------------
 2/9      1,5,10-32,101-120,150,200,250,300,400,500,600,700,800,900,1000

Port      Vlans in spanning tree forwarding state and not pruned
--------  ---------------------------------------------------------------------
 2/9      5,10-32,101-120,150,200,250,300,400,500,600,700,800,900,1000
Console> (enable)
```

Configuring an ISL/802.1Q Negotiating Trunk Port

To configure a trunk port to negotiate the trunk encapsulation type (either ISL or 802.1Q), perform this task in privileged mode:

	Task	Command
Step 1	Configure a port to negotiate the trunk encapsulation type.	**set trunk** *mod/port* [**on** | **desirable** | **auto** | **nonegotiate**] **negotiate**
Step 2	Verify the trunking configuration.	**show trunk** [*mod/port*]

This example shows how to configure a port to negotiate the encapsulation type and how to verify the trunk configuration. This example assumes that the neighboring port is in **auto** mode with encapsulation set to **isl** or **negotiate**.

```
Console> (enable) set trunk 4/11 desirable negotiate
Port(s) 4/11 trunk mode set to desirable.
Port(s) 4/11 trunk type set to negotiate.
```

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0795
Fls:
3701
Doc:

```
Console> (enable) show trunk 4/11
Port      Mode         Encapsulation  Status        Native vlan
--------  -----------  -------------  ------------  -----------
 4/11     desirable    n-isl          trunking      1

Port      Vlans allowed on trunk
--------  ---------------------------------------------------------------------
 4/11     1-1005,1025-4094

Port      Vlans allowed and active in management domain
--------  ---------------------------------------------------------------------
 4/11     1,5,10-32,55,101-120,998-1000

Port      Vlans in spanning tree forwarding state and not pruned
--------  ---------------------------------------------------------------------
 4/11     1,5,10-32,55,101-120,998-1000
Console> (enable)
```

Defining the Allowed VLANs on a Trunk

When you configure a trunk port, all VLANs are added to the allowed VLANs list for that trunk. However, you can remove VLANs from the allowed list to prevent traffic for those VLANs from passing over the trunk.

Note When you first configure a port as a trunk, entering the **set trunk** command always adds all VLANs to the allowed VLAN list for the trunk, even if you specify a VLAN range (any specified VLAN range is ignored). To modify the allowed VLANs list, use a combination of the **clear trunk** and **set trunk** commands to specify the allowed VLANs.

To define the allowed VLAN list for a trunk port, perform this task in privileged mode:

	Task	Command
Step 1	Remove VLANs from the allowed VLANs list for a trunk.	**clear trunk** *mod/port vlans*
Step 2	(Optional) Add specific VLANs to the allowed VLANs list for a trunk.	**set trunk** *mod/port vlans*
Step 3	Verify the allowed VLAN list for the trunk.	**show trunk** [*mod/port*]

This example shows how to define the allowed VLANs list to allow VLANs 1–100, VLANs 500–1005, and VLAN 2500 on trunk port 1/1 and how to verify the allowed VLAN list for the trunk:

```
Console> (enable) clear trunk 1/1 101-499
Removing Vlan(s) 101-499 from allowed list.
Port 1/1 allowed vlans modified to 1-100,500-1005.
Console> (enable) set trunk 1/1 2500
Adding vlans 2500 to allowed list.
Port(s) 1/1 allowed vlans modified to 1-100,500-1005,2500.
Console> (enable) show trunk 1/1
Port      Mode         Encapsulation  Status        Native vlan
--------  -----------  -------------  ------------  -----------
 1/1      desirable    isl            trunking      1
Port      Vlans allowed on trunk
--------  ---------------------------------------------------------------------
 1/1      1-100, 500-1005,2500
```

```
Port      Vlans allowed and active in management domain
--------  ---------------------------------------------------------------
 1/1      1,521-524
Port      Vlans in spanning tree forwarding state and not pruned
--------  ---------------------------------------------------------------
 1/1      1,521-524
Console> (enable)
```

3243
21

Disabling a Trunk Port

To turn off trunking on a port, perform this task in privileged mode:

	Task	Command
Step 1	Turn off trunking on a port.	**set trunk** *mod/port* **off**
Step 2	Verify the trunking configuration.	**show trunk** [*mod/port*]

To return a port to the default trunk type and mode for that port type, perform this task in privileged mode:

	Task	Command
Step 1	Return the port to the default trunking type and mode for that port type.	**clear trunk** *mod/port*
Step 2	Verify the trunking configuration.	**show trunk** [*mod/port*]

Example VLAN Trunk Configurations

This section contains example VLAN trunk configurations:

- ISL Trunk Configuration Example, page 5-9
- ISL Trunk Over EtherChannel Link Example, page 5-11
- 802.1Q Trunk Over EtherChannel Link Example, page 5-13
- Load-Sharing VLAN Traffic Over Parallel Trunks Example, page 5-17

ISL Trunk Configuration Example

This example shows how to configure an ISL trunk between two switches and how to limit the allowed VLANs on the trunk to VLAN 1 and VLANs 520–530.

In this example, port 1/1 on Switch 1 is connected to a Fast Ethernet port on another switch. Both ports are in their default state, with the trunk mode set to **auto** (for more information, see the "Default Trunk Configuration" section on page 5-5).

ECT/NE/03/0796-CN
CPMI - CORREIOS
0796
Fls:
3701
Doc:

Step 1 Configure port 1/1 on Switch 1 as an ISL trunk port by entering the **set trunk** command. By specifying the **desirable** keyword, the trunk is automatically negotiated with the neighboring port (port 1/2 on Switch 2). ISL encapsulation is assumed based on the hardware type.

```
Switch1> (enable) set trunk 1/1 desirable
Port(s) 1/1 trunk mode set to desirable.
Switch1> (enable) 06/18/1998,12:20:23:DTP-5:Port 1/1 has become isl trunk
06/18/1998,12:20:23:PAGP-5:Port 1/1 left bridge port 1/1.
06/18/1998,12:20:23:PAGP-5:Port 1/1 joined bridge port 1/1.
Switch1> (enable)
```

Step 2 Check the configuration by entering the **show trunk** command. The Status field in the screen output indicates that port 1/1 is trunking.

```
Switch1> (enable) show trunk 1/1
Port      Mode         Encapsulation  Status        Native vlan
--------  -----------  -------------  ------------  -----------
 1/1      desirable    isl            trunking      1
Port      Vlans allowed on trunk
--------  ---------------------------------------------------------------------
 1/1      1-1005, 1025-4094
Port      Vlans allowed and active in management domain
--------  ---------------------------------------------------------------------
 1/1      1,521-524
Port      Vlans in spanning tree forwarding state and not pruned
--------  ---------------------------------------------------------------------
 1/1
Switch1> (enable)
```

Step 3 Define the allowed VLAN list for the trunk by entering the **clear trunk** command to remove the VLANs that should not pass traffic over the trunk link.

```
Switch1> (enable) clear trunk 1/1 2-519
Removing Vlan(s) 2-519 from allowed list.
Port 1/1 allowed vlans modified to 1,520-1005.
Switch1> (enable) clear trunk 1/1 531-1005
Removing Vlan(s) 531-1005 from allowed list.
Port 1/1 allowed vlans modified to 1,520-530.
Switch1> (enable) show trunk 1/1
Port      Mode         Encapsulation  Status        Native vlan
--------  -----------  -------------  ------------  -----------
 1/1      desirable    isl            trunking      1
Port      Vlans allowed on trunk
--------  ---------------------------------------------------------------------
 1/1      1,520-530
Port      Vlans allowed and active in management domain
--------  ---------------------------------------------------------------------
 1/1      1,521-524
Port      Vlans in spanning tree forwarding state and not pruned
--------  ---------------------------------------------------------------------
 1/1      1,521-524
Switch1> (enable)
```

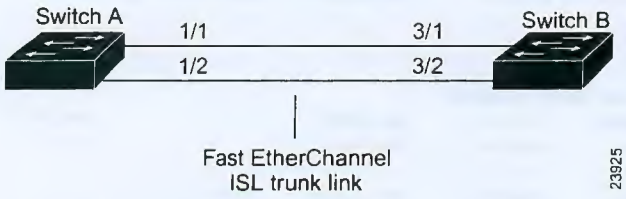
Step 4 Verify connectivity across the trunk by entering the **ping** command.

```
Switch1> (enable) ping switch2
switch2 is alive
Switch1> (enable)
```

ISL Trunk Over EtherChannel Link Example

This example shows how to configure an ISL trunk over an EtherChannel link between two switches. Figure 5-1 shows two switches connected through two 100BASE-TX Fast Ethernet ports.

Figure 5-1 ISL Trunk Over Fast EtherChannel Link



This example shows how to configure the switches to form a two-port EtherChannel bundle and then configure the EtherChannel bundle as an ISL trunk link.

Step 1 Confirm the channeling and trunking status of the switches by entering the **show port channel** and **show trunk** commands.

```
Switch_A> (enable) show port channel
No ports channelling
Switch_A> (enable) show trunk
No ports trunking.
Switch_A> (enable)

Switch_B> (enable) show port channel
No ports channelling
Switch_B> (enable) show trunk
No ports trunking.
Switch_B> (enable)
```

Step 2 Configure the ports on Switch A to negotiate an EtherChannel bundle with the neighboring switch by entering the **set port channel** command. This example assumes that the neighboring ports on Switch B are in EtherChannel **auto** mode. The system logging messages provide information about the formation of the EtherChannel bundle.

```
Switch_A> (enable) set port channel 1/1-2 desirable
Port(s) 1/1-2 channel mode set to desirable.
Switch_A> (enable) %PAGP-5-PORTFROMSTP:Port 1/1 left bridge port 1/1
%PAGP-5-PORTFROMSTP:Port 1/2 left bridge port 1/2
%PAGP-5-PORTFROMSTP:Port 1/2 left bridge port 1/2
%PAGP-5-PORTTOSTP:Port 1/1 joined bridge port 1/1-2
%PAGP-5-PORTTOSTP:Port 1/2 joined bridge port 1/1-2

Switch_B> (enable) %PAGP-5-PORTFROMSTP:Port 3/1 left bridge port 3/1
%PAGP-5-PORTFROMSTP:Port 3/2 left bridge port 3/2
%PAGP-5-PORTFROMSTP:Port 3/2 left bridge port 3/2
%PAGP-5-PORTTOSTP:Port 3/1 joined bridge port 3/1-2
%PAGP-5-PORTTOSTP:Port 3/2 joined bridge port 3/1-2
```

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0797
Fls:
Doc: 3701

Step 3 After the EtherChannel bundle is negotiated, verify the configuration by entering the **show port channel** command.

```
Switch_A> (enable) show port channel
Port  Status      Channel    Channel     Neighbor                  Neighbor
                  mode       status      device                    port
----- ----------- ---------- ----------- ------------------------- ----------
 1/1  connected   desirable  channel     WS-C5000     009979082(Sw  3/1
 1/2  connected   desirable  channel     WS-C5000     009979082(Sw  3/2
----- ----------- ---------- ----------- ------------------------- ----------
Switch_A> (enable)

Switch_B> (enable) show port channel
Port  Status      Channel    Channel     Neighbor                  Neighbor
                  mode       status      device                    port
----- ----------- ---------- ----------- ------------------------- ----------
 3/1  connected   auto       channel     WS-C5500     069003103(Sw  1/1
 3/2  connected   auto       channel     WS-C5500     069003103(Sw  1/2
----- ----------- ---------- ----------- ------------------------- ----------
Switch_B> (enable)
```

Step 4 Configure one of the ports in the EtherChannel bundle to negotiate an ISL trunk by entering the **set trunk** command.

The configuration is applied to all of the ports in the bundle. This example assumes that the neighboring ports on Switch B are configured to use **isl** or **negotiate** encapsulation and are in **auto** trunk mode. The system logging messages provide information about the formation of the ISL trunk.

```
Switch_A> (enable) set trunk 1/1 desirable isl
Port(s) 1/1-2 trunk mode set to desirable.
Port(s) 1/1-2 trunk type set to isl.
Switch_A> (enable) %DTP-5-TRUNKPORTON:Port 1/1 has become isl trunk
%DTP-5-TRUNKPORTON:Port 1/2 has become isl trunk
%PAGP-5-PORTFROMSTP:Port 1/1 left bridge port 1/1-2
%PAGP-5-PORTFROMSTP:Port 1/2 left bridge port 1/1-2
%PAGP-5-PORTTOSTP:Port 1/1 joined bridge port 1/1-2
%PAGP-5-PORTTOSTP:Port 1/2 joined bridge port 1/1-2

Switch_B> (enable) %DTP-5-TRUNKPORTON:Port 3/1 has become isl trunk
%DTP-5-TRUNKPORTON:Port 3/2 has become isl trunk
%PAGP-5-PORTFROMSTP:Port 3/1 left bridge port 3/1-2
%PAGP-5-PORTFROMSTP:Port 3/2 left bridge port 3/1-2
%PAGP-5-PORTTOSTP:Port 3/1 joined bridge port 3/1-2
%PAGP-5-PORTTOSTP:Port 3/2 joined bridge port 3/1-2
```

Step 5 After the ISL trunk link is negotiated, verify the configuration by entering the **show trunk** command.

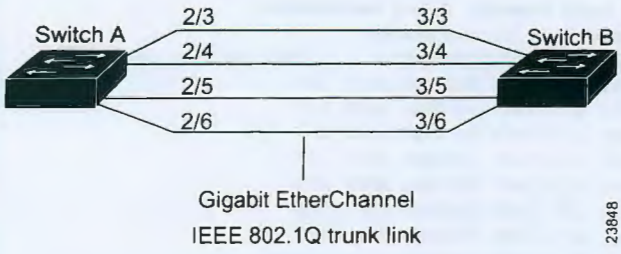
```
Switch_A> (enable) show trunk
Port      Mode         Encapsulation  Status        Native vlan
--------  -----------  -------------  ------------  -----------
 1/1      desirable    isl            trunking      1
 1/2      desirable    isl            trunking      1

Port      Vlans allowed on trunk
--------  ---------------------------------------------------------------------
 1/1      1-1005, 1025-4094
 1/2      1-1005, 1025-4094

Port      Vlans allowed and active in management domain
--------  ---------------------------------------------------------------------
 1/1      1-5,10,20,50,152,200,300,400,500,521-524,570,850,917,999
 1/2      1-5,10,20,50,152,200,300,400,500,521-524,570,850,917,999
```

```
Port      Vlans in spanning tree forwarding state and not pruned
--------  ---------------------------------------------------------------
 1/1      1-5,10,20,50,152,200,300,400,500,521-524,570,850,917,999
 1/2      1-5,10,20,50,152,200,300,400,500,521-524,570,850,917,999
Switch_A> (enable)

Switch_B> (enable) show trunk
Port      Mode         Encapsulation  Status        Native vlan
--------  -----------  -------------  ------------  -----------
 3/1      auto         isl            trunking      1
 3/2      auto         isl            trunking      1

Port      Vlans allowed on trunk
--------  ---------------------------------------------------------------
 3/1      1-1005, 1025-4094
 3/2      1-1005, 1025-4094

Port      Vlans allowed and active in management domain
--------  ---------------------------------------------------------------
 3/1      1-5,10,20,50,152,200,300,400,500,521-524,570,850,917,999
 3/2      1-5,10,20,50,152,200,300,400,500,521-524,570,850,917,999
Port      Vlans in spanning tree forwarding state and not pruned
--------  ---------------------------------------------------------------
 3/1      1-5,10,20,50,152,200,300,400,500,521-524,570,801,850,917,999
 3/2      1-5,10,20,50,152,200,300,400,500,521-524,570,801,850,917,999
Switch_B> (enable)
```

802.1Q Trunk Over EtherChannel Link Example

This example shows how to configure an 802.1Q trunk over an EtherChannel link between two switches. Figure 5-2 shows two switches connected through four 1000BASE-SX Gigabit Ethernet ports.

Figure 5-2 802.1Q Trunk Over EtherChannel Link



This example shows how to configure the switches to form a four-port EtherChannel bundle and then configure the EtherChannel bundle as an 802.1Q trunk link.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 0798
Doc: 3701

Step 1 Make sure all ports on both Switch A and Switch B are assigned to the same VLAN by entering the **set vlan** command. This VLAN is used as the 802.1Q native VLAN for the trunk. In this example, all ports are configured as members of VLAN 1.

```
Switch_A> (enable) set vlan 1 2/3-6
VLAN  Mod/Ports
---- ----------------------
1     2/1-6

Switch_A> (enable)

Switch_B> (enable) set vlan 1 3/3-6
VLAN  Mod/Ports
---- ----------------------
1     3/1-6

Switch_B> (enable)
```

Step 2 Confirm the channeling and trunking status of the switches by entering the **show port channel** and **show trunk** commands.

```
Switch_A> (enable) show port channel
No ports channelling
Switch_A> (enable) show trunk
No ports trunking.
Switch_A> (enable)

Switch_B> (enable) show port channel
No ports channelling
Switch_B> (enable) show trunk
No ports trunking.
Switch_B> (enable)
```

Step 3 Configure the ports on Switch A to negotiate an EtherChannel bundle with the neighboring switch by entering the **set port channel** command. This example assumes that the neighboring ports on Switch B are in EtherChannel **auto** mode. The system logging messages provide information about the formation of the EtherChannel bundle.

```
Switch_A> (enable) set port channel 2/3-6 desirable
Port(s) 2/3-6 channel mode set to desirable.
Switch_A> (enable) %PAGP-5-PORTFROMSTP:Port 2/3 left bridge port 2/3
%PAGP-5-PORTFROMSTP:Port 2/4 left bridge port 2/4
%PAGP-5-PORTFROMSTP:Port 2/5 left bridge port 2/5
%PAGP-5-PORTFROMSTP:Port 2/6 left bridge port 2/6
%PAGP-5-PORTFROMSTP:Port 2/4 left bridge port 2/4
%PAGP-5-PORTFROMSTP:Port 2/5 left bridge port 2/5
%PAGP-5-PORTFROMSTP:Port 2/6 left bridge port 2/6
%PAGP-5-PORTFROMSTP:Port 2/3 left bridge port 2/3
%PAGP-5-PORTTOSTP:Port 2/3 joined bridge port 2/3-6
%PAGP-5-PORTTOSTP:Port 2/4 joined bridge port 2/3-6
%PAGP-5-PORTTOSTP:Port 2/5 joined bridge port 2/3-6
%PAGP-5-PORTTOSTP:Port 2/6 joined bridge port 2/3-6

Switch_B> (enable) %PAGP-5-PORTFROMSTP:Port 3/3 left bridge port 3/3
%PAGP-5-PORTFROMSTP:Port 3/4 left bridge port 3/4
%PAGP-5-PORTFROMSTP:Port 3/5 left bridge port 3/5
%PAGP-5-PORTFROMSTP:Port 3/6 left bridge port 3/6
%PAGP-5-PORTFROMSTP:Port 3/4 left bridge port 3/4
%PAGP-5-PORTFROMSTP:Port 3/5 left bridge port 3/5
%PAGP-5-PORTFROMSTP:Port 3/6 left bridge port 3/6
```

```
%PAGP-5-PORTFROMSTP:Port 3/3 left bridge port 3/3
%PAGP-5-PORTTOSTP:Port 3/3 joined bridge port 3/3-6
%PAGP-5-PORTTOSTP:Port 3/4 joined bridge port 3/3-6
%PAGP-5-PORTTOSTP:Port 3/5 joined bridge port 3/3-6
%PAGP-5-PORTTOSTP:Port 3/6 joined bridge port 3/3-6
```

Step 4 After the EtherChannel bundle is negotiated, verify the configuration by entering the **show port channel** command.

```
Switch_A> (enable) show port channel
Port  Status      Channel    Channel     Neighbor                  Neighbor
                  mode       status      device                    port
----- ----------- ---------- ----------- ------------------------- ----------
 2/3  connected   desirable  channel     WS-C4003    JAB023806(Sw  2/3
 2/4  connected   desirable  channel     WS-C4003    JAB023806(Sw  2/4
 2/5  connected   desirable  channel     WS-C4003    JAB023806(Sw  2/5
 2/6  connected   desirable  channel     WS-C4003    JAB023806(Sw  2/6
----- ----------- ---------- ----------- ------------------------- ----------
Switch_A> (enable)

Switch_B> (enable) show port channel
Port  Status      Channel    Channel     Neighbor                  Neighbor
                  mode       status      device                    port
----- ----------- ---------- ----------- ------------------------- ----------
 3/3  connected   auto       channel     WS-C4003    JAB023806(Sw  2/3
 3/4  connected   auto       channel     WS-C4003    JAB023806(Sw  2/4
 3/5  connected   auto       channel     WS-C4003    JAB023806(Sw  2/5
 3/6  connected   auto       channel     WS-C4003    JAB023806(Sw  2/6
----- ----------- ---------- ----------- ------------------------- ----------
Switch_B> (enable)
```

Step 5 Configure one of the ports in the EtherChannel bundle to negotiate an 802.1Q trunk by entering the **set trunk** command. The configuration is applied to all of the ports in the bundle. This example assumes that the neighboring ports on Switch B are configured to use **dot1q** or **negotiate** encapsulation and are in **auto** trunk mode. The system logging messages provide information about the formation of the 802.1Q trunk.

```
Switch_A> (enable) set trunk 2/3 desirable dot1q
Port(s) 2/3-6 trunk mode set to desirable.
Port(s) 2/3-6 trunk type set to dot1q.
Switch_A> (enable) %DTP-5-TRUNKPORTON:Port 2/3 has become dot1q trunk
%DTP-5-TRUNKPORTON:Port 2/4 has become dot1q trunk
%PAGP-5-PORTFROMSTP:Port 2/3 left bridge port 2/3-6
%DTP-5-TRUNKPORTON:Port 2/5 has become dot1q trunk
%PAGP-5-PORTFROMSTP:Port 2/4 left bridge port 2/3-6
%PAGP-5-PORTFROMSTP:Port 2/5 left bridge port 2/3-6
%DTP-5-TRUNKPORTON:Port 2/6 has become dot1q trunk
%PAGP-5-PORTFROMSTP:Port 2/6 left bridge port 2/3-6
%PAGP-5-PORTFROMSTP:Port 2/3 left bridge port 2/3
%PAGP-5-PORTTOSTP:Port 2/3 joined bridge port 2/3-6
%PAGP-5-PORTTOSTP:Port 2/4 joined bridge port 2/3-6
%PAGP-5-PORTTOSTP:Port 2/5 joined bridge port 2/3-6
%PAGP-5-PORTTOSTP:Port 2/6 joined bridge port 2/3-6
Switch_B> (enable) %DTP-5-TRUNKPORTON:Port 3/3 has become dot1q trunk
%DTP-5-TRUNKPORTON:Port 3/4 has become dot1q trunk
%PAGP-5-PORTFROMSTP:Port 3/3 left bridge port 3/3-6
%PAGP-5-PORTFROMSTP:Port 3/4 left bridge port 3/3-6
%PAGP-5-PORTFROMSTP:Port 3/5 left bridge port 3/3-6
%PAGP-5-PORTFROMSTP:Port 3/6 left bridge port 3/3-6
%DTP-5-TRUNKPORTON:Port 3/5 has become dot1q trunk
%DTP-5-TRUNKPORTON:Port 3/6 has become dot1q trunk
%PAGP-5-PORTFROMSTP:Port 3/5 left bridge port 3/3-6
%PAGP-5-PORTFROMSTP:Port 3/6 left bridge port 3/3-6
```

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0799
Fls:
Doc: 3701

```
%PAGP-5-PORTTOSTP:Port 3/3 joined bridge port 3/3-6
%PAGP-5-PORTTOSTP:Port 3/4 joined bridge port 3/3-6
%PAGP-5-PORTTOSTP:Port 3/5 joined bridge port 3/3-6
%PAGP-5-PORTTOSTP:Port 3/6 joined bridge port 3/3-6
```

Step 6 After the 802.1Q trunk link is negotiated, verify the configuration by entering the **show trunk** command.

```
Switch_A> (enable) show trunk
Port      Mode         Encapsulation  Status        Native vlan
--------  -----------  -------------  ------------  -----------
 2/3      desirable    dot1q          trunking      1
 2/4      desirable    dot1q          trunking      1
 2/5      desirable    dot1q          trunking      1
 2/6      desirable    dot1q          trunking      1

Port      Vlans allowed on trunk
--------  ---------------------------------------------------------------------
 2/3      1-1005, 1025-4094
 2/4      1-1005, 1025-4094
 2/5      1-1005, 1025-4094
 2/6      1-1005, 1025-4094

Port      Vlans allowed and active in management domain
--------  ---------------------------------------------------------------------
 2/3      1-5,10,20,50,152,200,300,400,500,521-524,570,850,917,999
 2/4      1-5,10,20,50,152,200,300,400,500,521-524,570,850,917,999
 2/5      1-5,10,20,50,152,200,300,400,500,521-524,570,850,917,999
 2/6      1-5,10,20,50,152,200,300,400,500,521-524,570,850,917,999

Port      Vlans in spanning tree forwarding state and not pruned
--------  ---------------------------------------------------------------------
 2/3
 2/4
 2/5
 2/6
Switch_A> (enable)

Switch_B> (enable) show trunk
Port      Mode         Encapsulation  Status        Native vlan
--------  -----------  -------------  ------------  -----------
 3/3      auto         dot1q          trunking      1
 3/4      auto         dot1q          trunking      1
 3/5      auto         dot1q          trunking      1
 3/6      auto         dot1q          trunking      1

Port      Vlans allowed on trunk
--------  ---------------------------------------------------------------------
 3/3      1-1005, 1025-4094
 3/4      1-1005, 1025-4094
 3/5      1-1005, 1025-4094
 3/6      1-1005, 1025-4094

Port      Vlans allowed and active in management domain
--------  ---------------------------------------------------------------------
 3/3      1-5,10,20,50,152,200,300,400,500,521-524,570,850,917,999
 3/4      1-5,10,20,50,152,200,300,400,500,521-524,570,850,917,999
 3/5      1-5,10,20,50,152,200,300,400,500,521-524,570,850,917,999
 3/6      1-5,10,20,50,152,200,300,400,500,521-524,570,850,917,999
```

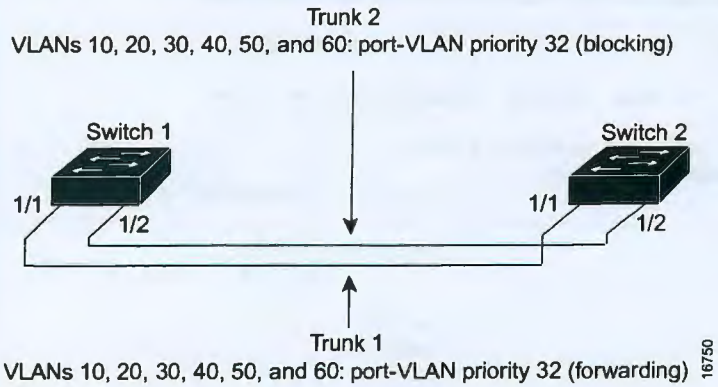
```
Port      Vlans in spanning tree forwarding state and not pruned
--------  ------------------------------------------------------------------
 3/3      1-5,10,20,50,152,200,300,400,500,521-524,570,850,917,999
 3/4      1-5,10,20,50,152,200,300,400,500,521-524,570,850,917,999
 3/5      1-5,10,20,50,152,200,300,400,500,521-524,570,850,917,999
 3/6      1-5,10,20,50,152,200,300,400,500,521-524,570,850,917,999
Switch_B> (enable)
```

Load-Sharing VLAN Traffic Over Parallel Trunks Example

Using spanning tree port-VLAN priorities, you can load-share VLAN traffic over parallel trunk ports so that traffic from some VLANs travels over one trunk, while traffic from other VLANs travels over the other trunk. This configuration allows traffic to be carried over both trunks simultaneously (instead of keeping one trunk in blocking mode), which reduces the total traffic carried over each trunk while still maintaining a fault-tolerant configuration.

Figure 5-3 shows a parallel trunk configuration between two switches, using the Fast Ethernet uplink ports on the supervisor engine.

Figure 5-3 Parallel Trunk Configuration Before Configuring VLAN-Traffic Load Sharing



By default, the port-VLAN priority for both trunks is equal (a value of 32). STP blocks port 1/2 (Trunk 2) for each VLAN on Switch 1 to prevent forwarding loops. Trunk 2 is not used to forward traffic unless Trunk 1 fails.

This example shows how to configure the switches so that traffic from multiple VLANs is load balanced over the parallel trunks.

Step 1 Configure a VTP domain on both Switch 1 and Switch 2 by entering the **set vtp** command so that the VLAN information configured on Switch 1 is learned by Switch 2. Make sure Switch 1 is a VTP server. You can configure Switch 2 as a VTP client or as a VTP server.

```
Switch_1> (enable) set vtp domain BigCorp mode server
VTP domain BigCorp modified
Switch_1> (enable)

Switch_2> (enable) set vtp domain BigCorp mode server
VTP domain BigCorp modified
Switch_2> (enable)
```

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0800
Fls:
Doc: 3701

Step 2 Create the VLANs on Switch 1 by entering the **set vlan** command. In this example, you see VLANs 10, 20, 30, 40, 50, and 60.

```
Switch_1> (enable) set vlan 10
Vlan 10 configuration successful
Switch_1> (enable) set vlan 20
Vlan 20 configuration successful
Switch_1> (enable) set vlan 30
Vlan 30 configuration successful
Switch_1> (enable) set vlan 40
Vlan 40 configuration successful
Switch_1> (enable) set vlan 50
Vlan 50 configuration successful
Switch_1> (enable) set vlan 60
Vlan 60 configuration successful
Switch_1> (enable)
```

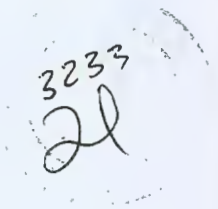
Step 3 Verify the VTP and VLAN configuration on Switch 1 by entering the **show vtp domain** and **show vlan** commands.

```
Switch_1> (enable) show vtp domain
Domain Name                    Domain Index VTP Version Local Mode  Password
------------------------------ ------------ ----------- ----------- ----------
BigCorp                        1            2           server      -

Vlan-count Max-vlan-storage Config Revision Notifications
---------- --------------- --------------- -------------
11         1023            13              disabled

Last Updater    V2 Mode  Pruning  PruneEligible on Vlans
--------------- -------- -------- -------------------------
172.20.52.10    disabled enabled  2-1000
Switch_1> (enable) show vlan
VLAN Name                           Status    Mod/Ports, Vlans
---- ------------------------------ --------- ---------------------------
1    default                        active    1/1-2
                                              2/1-12
                                              5/1-2
10   VLAN0010                       active
20   VLAN0020                       active
30   VLAN0030                       active
40   VLAN0040                       active
50   VLAN0050                       active
60   VLAN0060                       active
1002 fddi-default                   active
1003 token-ring-default             active
1004 fddinet-default                active
1005 trnet-default                  active
.
.
.

Switch_1> (enable)
```

Step 4 Configure the supervisor engine uplinks on Switch 1 as ISL trunk ports by entering the **set trunk** command. Specifying the **desirable** mode on the Switch 1 ports causes the ports on Switch 2 to negotiate to become trunk links (assuming that the Switch 2 uplinks are in the default **auto** mode).

```
Switch_1> (enable) set trunk 1/1 desirable
Port(s) 1/1 trunk mode set to desirable.
Switch_1> (enable) 04/21/1998,03:05:05:DISL-5:Port 1/1 has become isl trunk
```

```
Switch_1> (enable) set trunk 1/2 desirable
Port(s) 1/2 trunk mode set to desirable.
Switch_1> (enable) 04/21/1998,03:05:13:DISL-5:Port 1/2 has become isl trunk
```



Step 5 Verify that the trunk links are up by entering the **show trunk** command.

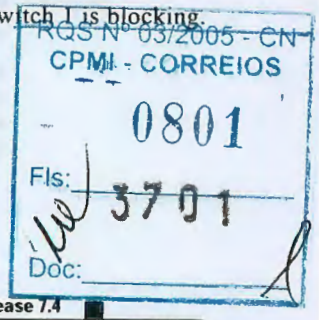
```
Switch_1> (enable) show trunk 1
Port      Mode         Encapsulation  Status        Native vlan
--------  -----------  -------------  ------------  -----------
 1/1      desirable    isl            trunking      1
 1/2      desirable    isl            trunking      1

Port      Vlans allowed on trunk
--------  ---------------------------------------------------------------------
 1/1      1-1005, 1025-4094
 1/2      1-1005, 1025-4094

Port      Vlans allowed and active in management domain
--------  ---------------------------------------------------------------------
 1/1      1,10,20,30,40,50,60
 1/2      1,10,20,30,40,50,60

Port      Vlans in spanning tree forwarding state and not pruned
--------  ---------------------------------------------------------------------
 1/1
 1/2
Switch_1> (enable)
```

Step 6 Note that when the trunk links come up, VTP passes the VTP and VLAN configuration to Switch 2. Verify that Switch 2 has learned the VLAN configuration by entering the **show vlan** command on Switch 2.

```
Switch_2> (enable) show vlan
VLAN Name                             Status    Mod/Ports, Vlans
---- -------------------------------- --------- -------------------------
1    default                          active
10   VLAN0010                         active
20   VLAN0020                         active
30   VLAN0030                         active
40   VLAN0040                         active
50   VLAN0050                         active
60   VLAN0060                         active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active

<...output truncated...>

Switch_2> (enable)
```

Step 7 Note that spanning tree takes one to two minutes to converge. After the network stabilizes, check the spanning tree state of each trunk port on Switch 1 by entering the **show spantree** command.

Trunk 1 is forwarding for all VLANs. Trunk 2 is blocking for all VLANs. On Switch 2, both trunks are forwarding for all VLANs, but no traffic passes over Trunk 2 because port 1/2 on Switch 1 is blocking.



```
Switch_1> (enable) show spantree 1/1
Port      Vlan  Port-State     Cost   Priority  Fast-Start  Group-method
--------- ----  -------------  -----  --------  ----------  ------------
 1/1      1     forwarding        19        32   disabled
 1/1      10    forwarding        19        32   disabled
 1/1      20    forwarding        19        32   disabled
 1/1      30    forwarding        19        32   disabled
 1/1      40    forwarding        19        32   disabled
 1/1      50    forwarding        19        32   disabled
 1/1      60    forwarding        19        32   disabled
 1/1      1003  not-connected     19        32   disabled
 1/1      1005  not-connected     19         4   disabled
Switch_1> (enable) show spantree 1/2
Port      Vlan  Port-State     Cost   Priority  Fast-Start  Group-method
--------- ----  -------------  -----  --------  ----------  ------------
 1/2      1     blocking          19        32   disabled
 1/2      10    blocking          19        32   disabled
 1/2      20    blocking          19        32   disabled
 1/2      30    blocking          19        32   disabled
 1/2      40    blocking          19        32   disabled
 1/2      50    blocking          19        32   disabled
 1/2      60    blocking          19        32   disabled
 1/2      1003  not-connected     19        32   disabled
 1/2      1005  not-connected     19         4   disabled
Switch_1> (enable)
```

Step 8 Divide the configured VLANs into two groups. You might want traffic from half of the VLANs to go over one trunk link and half over the other, or if one VLAN has heavier traffic than the others, you can forward traffic from that VLAN over one trunk and traffic from the other VLANs over the other trunk link.

Note In the following steps, VLANs 10, 20, and 30 (Group 1) are forwarded over Trunk 1, and VLANs 40, 50, and 60 (Group 2) are forwarded over Trunk 2.

Step 9 On Switch 1, change the port-VLAN priority for the Group 1 VLANs on Trunk 1 (port 1/1) to an integer value lower than the default of 32 by entering the **set spantree portvlanpri** command.

```
Switch_1> (enable) set spantree portvlanpri 1/1 1 10
Port 1/1 vlans 1-9,11-1004 using portpri 32.
Port 1/1 vlans 10 using portpri 1.
Port 1/1 vlans 1005 using portpri 4.
Switch_1> (enable) set spantree portvlanpri 1/1 1 20
Port 1/1 vlans 1-9,11-19,21-1004 using portpri 32.
Port 1/1 vlans 10,20 using portpri 1.
Port 1/1 vlans 1005 using portpri 4.
Switch_1> (enable) set spantree portvlanpri 1/1 1 30
Port 1/1 vlans 1-9,11-19,21-29,31-1004 using portpri 32.
Port 1/1 vlans 10,20,30 using portpri 1.
Port 1/1 vlans 1005 using portpri 4.
Switch_1> (enable)
```

Step 10 On Switch 1, change the port-VLAN priority for the Group 2 VLANs on Trunk 2 (port 1/2) to an integer value lower than the default of 32 by entering the **set spantree portvlanpri** command.

```
Switch_1> (enable) set spantree portvlanpri 1/2 1 40
Port 1/2 vlans 1-39,41-1004 using portpri 32.
Port 1/2 vlans 40 using portpri 1.
Port 1/2 vlans 1005 using portpri 4.
```

```
Switch_1> (enable) set spantree portvlanpri 1/2 1 50
Port 1/2 vlans 1-39,41-49,51-1004 using portpri 32.
Port 1/2 vlans 40,50 using portpri 1.
Port 1/2 vlans 1005 using portpri 4.
Switch_1> (enable) set spantree portvlanpri 1/2 1 60
Port 1/2 vlans 1-39,41-49,51-59,61-1004 using portpri 32.
Port 1/2 vlans 40,50,60 using portpri 1.
Port 1/2 vlans 1005 using portpri 4.
Switch_1> (enable)
```

Step 11 On Switch 2, change the port-VLAN priority for the Group 1 VLANs on Trunk 1 (port 1/1) to the same value you configured for those VLANs on Switch 1 by entering the **set spantree portvlanpri** command.

Caution The port-VLAN priority for each VLAN must be equal on both ends of the link.

```
Switch_2> (enable) set spantree portvlanpri 1/1 1 10
Port 1/1 vlans 1-9,11-1004 using portpri 32.
Port 1/1 vlans 10 using portpri 1.
Port 1/1 vlans 1005 using portpri 4.
Switch_2> (enable) set spantree portvlanpri 1/1 1 20
Port 1/1 vlans 1-9,11-19,21-1004 using portpri 32.
Port 1/1 vlans 10,20 using portpri 1.
Port 1/1 vlans 1005 using portpri 4.
Switch_2> (enable) set spantree portvlanpri 1/1 1 30
Port 1/1 vlans 1-9,11-19,21-29,31-1004 using portpri 32.
Port 1/1 vlans 10,20,30 using portpri 1.
Port 1/1 vlans 1005 using portpri 4.
Switch_2> (enable)
```

Step 12 On Switch 2, change the port-VLAN priority for the Group 2 VLANs on Trunk 2 (port 1/2) to the same value you configured for those VLANs on Switch 1 by entering the **set spantree portvlanpri** command.

```
Switch_2> (enable) set spantree portvlanpri 1/2 1 40
Port 1/2 vlans 1-39,41-1004 using portpri 32.
Port 1/2 vlans 40 using portpri 1.
Port 1/2 vlans 1005 using portpri 4.
Switch_2> (enable) set spantree portvlanpri 1/2 1 50
Port 1/2 vlans 1-39,41-49,51-1004 using portpri 32.
Port 1/2 vlans 40,50 using portpri 1.
Port 1/2 vlans 1005 using portpri 4.
Switch_2> (enable) set spantree portvlanpri 1/2 1 60
Port 1/2 vlans 1-39,41-49,51-59,61-1004 using portpri 32.
Port 1/2 vlans 40,50,60 using portpri 1.
Port 1/2 vlans 1005 using portpri 4.
Switch_2> (enable)
```

Note When you have configured the port-VLAN priorities on both ends of the link, the spanning tree converges to use the new configuration.

Step 13 Check the spanning tree port states on Switch 1 by entering the **show spantree** command. The Group 1 VLANs should forward on Trunk 1 and block on Trunk 2. The Group 2 VLANs should block on Trunk 1 and forward on Trunk 2.

3231
RQS Nº 03/2005 - CN
CPMI - CORREIOS
0802
Fls:
Doc: 3701

```
Switch_1> (enable) show spantree 1/1
Port      Vlan  Port-State     Cost   Priority  Fast-Start  Group-method
--------- ----  -------------  -----  --------  ----------  ------------
 1/1      1     forwarding        19        32   disabled
 1/1      10    forwarding        19         1   disabled
 1/1      20    forwarding        19         1   disabled
 1/1      30    forwarding        19         1   disabled
 1/1      40    blocking          19        32   disabled
 1/1      50    blocking          19        32   disabled
 1/1      60    blocking          19        32   disabled
 1/1      1003  not-connected     19        32   disabled
 1/1      1005  not-connected     19         4   disabled
Switch_1> (enable) show spantree 1/2
Port      Vlan  Port-State     Cost   Priority  Fast-Start  Group-method
--------- ----  -------------  -----  --------  ----------  ------------
 1/2      1     blocking          19        32   disabled
 1/2      10    blocking          19        32   disabled
 1/2      20    blocking          19        32   disabled
 1/2      30    blocking          19        32   disabled
 1/2      40    forwarding        19         1   disabled
 1/2      50    forwarding        19         1   disabled
 1/2      60    forwarding        19         1   disabled
 1/2      1003  not-connected     19        32   disabled
 1/2      1005  not-connected     19         4   disabled
Switch_1> (enable)
```

Figure 5-4 shows the network after you configure VLAN traffic load sharing.

Figure 5-4 Parallel Trunk Configuration After Configuring VLAN-Traffic Load Sharing

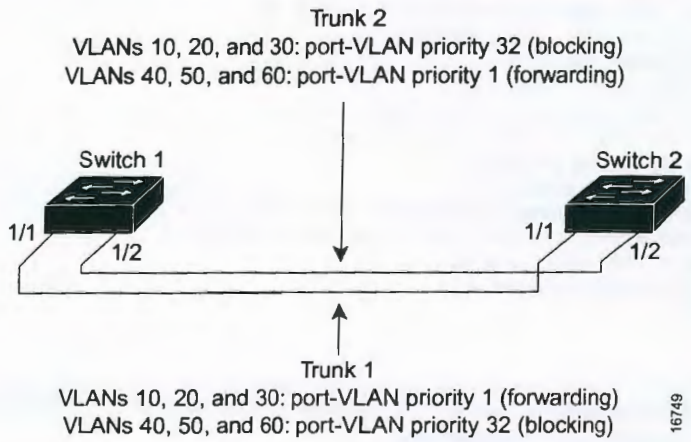


Figure 5-4 shows that both trunks are utilized when the network is operating normally; if one trunk link fails, the other trunk link acts as an alternate forwarding path for the traffic previously traveling over the failed link.

If Trunk 1 fails in the network shown in Figure 5-4, STP reconverges to use Trunk 2 to forward traffic from all the VLANs, as shown in this example:

```
Switch_1> (enable) 04/21/1998,03:15:40:DISL-5:Port 1/1 has become non-trunk

Switch_1> (enable) show spantree 1/1
Port      Vlan  Port-State     Cost   Priority  Fast-Start  Group-method
--------- ----  -------------  -----  --------  ----------  ------------
 1/1      1     not-connected     19        32   disabled
Switch_1> (enable) show spantree 1/2
Port      Vlan  Port-State     Cost   Priority  Fast-Start  Group-method
--------- ----  -------------  -----  --------  ----------  ------------
 1/2      1     learning          19        32   disabled
 1/2      10    learning          19        32   disabled
 1/2      20    learning          19        32   disabled
 1/2      30    learning          19        32   disabled
 1/2      40    forwarding        19         1   disabled
 1/2      50    forwarding        19         1   disabled
 1/2      60    forwarding        19         1   disabled
 1/2      1003  not-connected     19        32   disabled
 1/2      1005  not-connected     19         4   disabled
Switch_1> (enable) show spantree 1/2
Port      Vlan  Port-State     Cost   Priority  Fast-Start  Group-method
--------- ----  -------------  -----  --------  ----------  ------------
 1/2      1     forwarding        19        32   disabled
 1/2      10    forwarding        19        32   disabled
 1/2      20    forwarding        19        32   disabled
 1/2      30    forwarding        19        32   disabled
 1/2      40    forwarding        19         1   disabled
 1/2      50    forwarding        19         1   disabled
 1/2      60    forwarding        19         1   disabled
 1/2      1003  not-connected     19        32   disabled
 1/2      1005  not-connected     19         4   disabled
Switch_1> (enable)
```

Disabling VLAN 1 on Trunks

On the Catalyst 6500 series switches, VLAN 1 is enabled by default to allow control protocols to transmit and receive packets across the network topology. However, when VLAN 1 is enabled on trunk links in a large complex network, the impact of broadcast storms increases. Because spanning tree applies to the entire network, spanning tree loops might increase when you enable VLAN 1 on all trunk links. To prevent this scenario, you can disable VLAN 1 on trunk interfaces.

When you disable VLAN 1 on a trunk interface, no user traffic is transmitted and received across that trunk interface, but the supervisor engine continues to transmit and receive packets from control protocols such as Cisco Discovery Protocol (CDP), VTP, Port Aggregation Protocol (PAgP), and DTP.

When a trunk port with VLAN 1 disabled becomes a nontrunk port, it is added to the native VLAN. If the native VLAN is VLAN 1, the port is enabled and added to VLAN 1.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 0803
Doc: 3701

Disabling VLAN 1 on a Trunk Link

To disable VLAN 1 on a trunk interface, perform this task in privileged mode:

	Task	Command
Step 1	Disable VLAN 1 on the trunk interface.	**clear trunk** *mod/port* [*vlan-range*]
Step 2	Verify the allowed VLAN list for the trunk.	**show trunk** [*mod/port*]

This example shows how to disable VLAN 1 on a trunk link and verify the configuration:

```
Console> (enable) clear trunk 8/1 1
Removing Vlan(s) 1 from allowed list.
Port  8/1 allowed vlans modified to 2-1005.
Console> (enable) show trunk 8/1
Port      Mode         Encapsulation  Status        Native vlan
--------  -----------  -------------  ------------  -----------
 8/1      on           isl            trunking      1

Port      Vlans allowed on trunk
--------  ---------------------------------------------------------------------
 8/1      2-1005, 1025-4094

Port      Vlans allowed and active in management domain
--------  ---------------------------------------------------------------------
 8/1      2-6,10,20,50,100,152,200,300,400,500,521,524,570,776,801-802,850,917,9
99,1003,1005

Port      Vlans in spanning tree forwarding state and not pruned
--------  ---------------------------------------------------------------------
 8/1      2-6,10,20,50,100,152,200,300,400,500,521,524,570,776,802,850,917,999,1
003,1005
Console> (enable) show config
```

Ap BR

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0804
Fls:
Doc: 3791

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

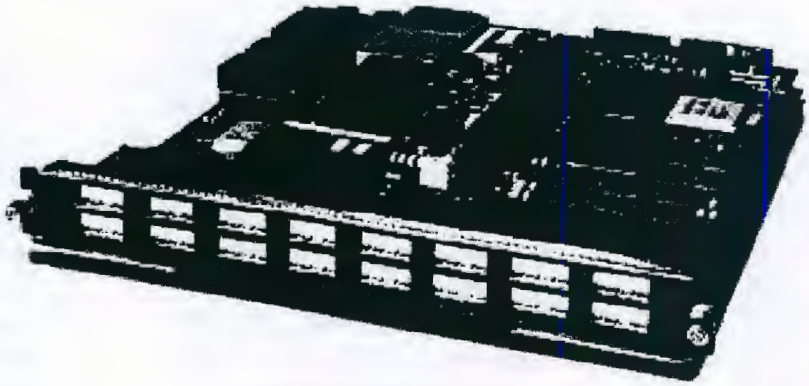
- High port densities—From 8 up to 16 ports per module, up to 256 ports per system
- Scalable and predictable performance—Provide a selection of switch fabric connections and throughput: 32 Gbps bandwidth/15 Mpps (Classic interface modules), 256 Gbps bandwidth/30 Mpps (CEF256 interface modules), and 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

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0805
Fls:
3701

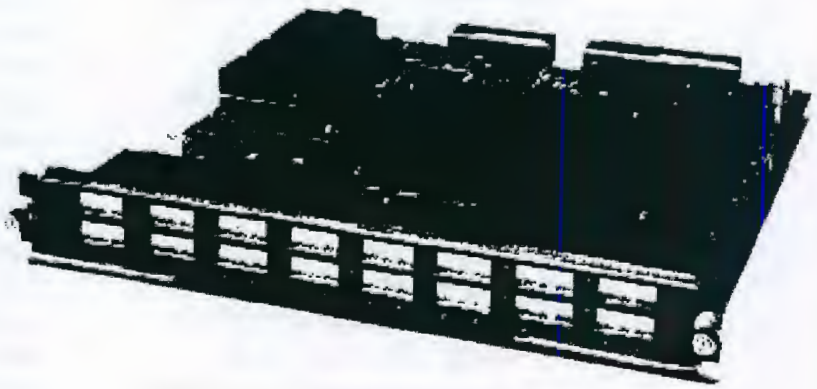
Cisco Systems, Inc.
All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

- 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



Cisco Systems, Inc.
All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

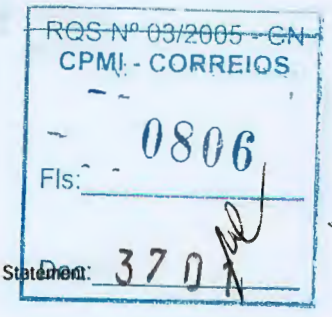
Gigabit Ethernet Applications

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



All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

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.

Cisco Systems, Inc.
All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

3223
21

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

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0807
Fls:
Doc: 3701

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

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

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

3221
2l

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

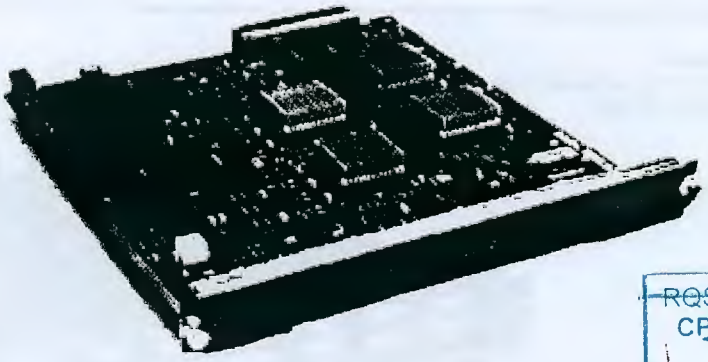
Distributed forwarding upgrade—None; Classic interface modules cannot be upgraded for distributed forwarding

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



RQS Nº 03/2005 - CN
CPMI - CORREIOS
0808
Fls:
3701
Doc:

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

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; requires a 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

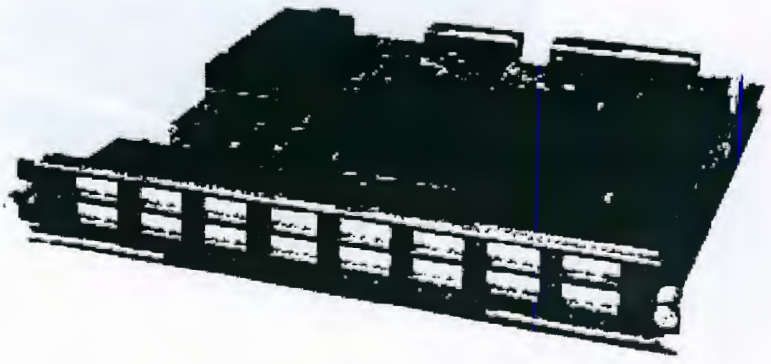
Port densities—192 ports: Catalyst 6513 chassis; 128 ports: Catalyst 6509 chassis

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



All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

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

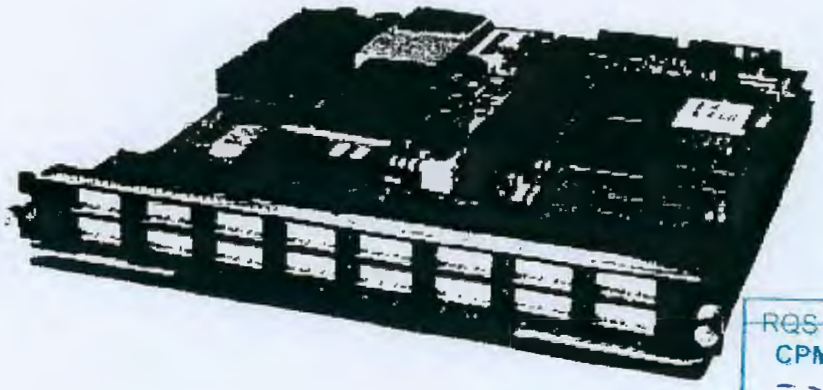
Distributed forwarding—Include a DFC when operating with Supervisor Engine 2 or a DFC3 when operating with Supervisor Engine 720

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



RQS Nº 03/2005 - CN -
CPMI - CORREIOS
0809
Doc: 3701

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

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

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

3218
21

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)

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0810
Fls:
3701
Doc:

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

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

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

3216
21

- 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

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0811
Fls:
Doc: 3701

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.

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

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 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

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

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Catalyst, Cisco, Cisco IOS, Cisco Systems, the Cisco Systems logo, EtherChannel, and SMARTnet are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0304R)

MH/LW4273 0403

AP BS

RQS-Nº 03/2005 - CN
CPMI - CORREIOS
0812
Fls:
Doc: 3701

3214

Close Window

Toolkit: Roll over tools t

Feedback | Help

CISCO SYSTEMS

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/VOX/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
c1700-k9o3sv8y7-mz.12.2-15.T	96	16	S17C7V8K9-12215T= S17C7V8K9-12215T	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
ddress Resolution Protocol (ARP)
DSL - 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
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 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

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0813
Fls:
3701
Doc:

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
Cisco IOS Telephony Service (ITS) Version 2.0
Cisco IOS Telephony Service (ITS) Version 2.01
Cisco IOS Telephony Service (ITS) Version 2.02
Cisco IOS Telephony Service (ITS) Version 2.1
ass Based Weighted Fair Queuing (CBWFQ)
lass-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
Context-Based Access Control (CBAC)
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
ICP 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
DLR Enhancements: PGM RFC-3208 Compliance
DNS based X.25 routing
DNS Lookups over an IPv6 Transport
Double Authentication
DTMF Relay for SIP Calls Using Named Telephone Events (NTE)
Dynamic Multiple Encapsulation for Dial-in over ISDN
Dynamic Multipoint VPN (DMVPN)

3213

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0814
Fls:
Doc: 3704

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
Firewall Authentication Proxy
Firewall Feature Set
Firewall Intrusion Detection (IDS) Signature Enhancements
Firewall Intrusion Detection System
ewall N2H2 Support
irewall Stateful Inspection of ICMP
Firewall Support for SIP
Firewall Support of SSL Encrypted HTTP Authentication Proxy Sign-on
Firewall Websense URL Filtering
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
Gateway Enhancements to Enable v4-v2 Interworking
neric 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)
Interactive Voice Response (IVR) Version 2.0

3213
2d

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0815
Fls:
3701
Doc:

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
ISDN Progress Indicator support for SIP using 183 Session Progress
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
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 VoIP Call Admission Control
MGCP VoIP Signaling
Microsoft Point-to-Point Compression (MPPC)
MLPPP with Link Fragmentation Interleave (LFI)
Modem PassThrough over Voice over IP
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 for SIP
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

3212
RQS Nº 03/2005 - CN
CPMI - CORREIOS
0816
Fls:
3701
Doc:

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
rcentage-Based Policing and Shaping
GM 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)
Port to Application Mapping (PAM)
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
PSTN Fallback
QoS Device Manager (QDM)
QoS for Virtual Private Networks
QoS Packet Marking
S 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

3211
2d

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0817
Fls:
Doc: 3701

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
SIP - Call Transfer Enhancements Using Refer Method
SIP - Call Transfer Using Refer Method
SIP - Configurable PSTN Cause Code Mapping
SIP - DNS SRV RFC2782 Compliance
SIP - Session Initiation Protocol for VoIP
SIP - Session Initiation Protocol for VoIP Enhancements
SIP Diversion Header Implementation for Redirecting Number
SIP Enhanced 180 Provisional Response Handling
SIP Extensions for Caller Identity and Privacy
SIP Gateway Support for the Bind Command
SIP Gateway support for Third Party Call Control
SIP Gateway Support of 'tel' URL
SIP Gateway Support of RSVP
SIP Intra-gateway Hairpinning
SIP INVITE Request with Malformed Via Header
SIP Redirect Processing Enhancement
SIP T.38 Fax Relay
SIP: Core SIP Technology Enhancements
SIP: ISDN Suspend/Resume Support
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
SRST: Survivable Remote Site Telephony Version 1.0
SRST: Survivable Remote Site Telephony Version 2.0
SRST: Survivable Remote Site Telephony Version 2.02
SRST: Survivable Remote Site Telephony Version 2.1
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.37 Store and Forward Fax
T.38 Fax Relay for VoIP H.323
T1 Channel Associated Signaling (CAS)
T1/E1 Voice PRI Q.931

3210
RQS Nº 03/2005 - CN
CPMI - CORREIOS
0818
Fls: 370
Doc:

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
irtual Router Redundancy Protocol (VRRP)
oice 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
25 over Frame Relay (Annex G)
.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

© 1992-2003 Cisco Systems, Inc. All rights reserved. Important Notices, Privacy Statement, and Trademarks of Cisco Systems, Inc.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0819
Fls:
Doc: 3701

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0820
Fls:
3701
Doc:

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

3205
2l

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0821
Fls:
Doc: 3701

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

3204
2l

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0822
Fls: 3701
Doc:

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

3203

RQS Nº 03/2005 - CN - CPMI - CORREIOS
0823
Fls:
3701
Doc:

To find out more about your selected release, you can use the Bug Toolkit

Close Window

© 1992-2003 Cisco Systems, Inc. All rights reserved. Important Notices, Privacy Statement, and Trademarks of Cisco Systems, Inc.

3202
20

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0824
Fls:
3701
Doc:

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0825
Fls:
3701
Doc:

Close Window

3201
21

Toolkit: Roll over tools

Feedback | Help

CISCO SYSTEMS

Software Advisor

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
`dditional Vendor-Proprietary RADIUS Attributes
.ddress 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

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0826
Fls:
3701
Doc:

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
NS Configuration Agent
NS 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
HCP 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
DLR 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

3200
21

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0827
Fls:
3701
Doc:

3199
21

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)

ROS Nº 03/2005 - CN
CPMI - CORREIOS
0828
Fls:
Doc: 3701

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

3198

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0829
Fls: 3701
Doc:

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

3197

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0830
Fls:
3701
Doc:

3196
2l

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
raffic Policing
ransparent 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
PDN 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

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0831
Fls:
1370
Doc:

3195
21

To find out more about your selected release, you can use the Bug Toolkit

Close Window

© 1992-2003 Cisco Systems, Inc. All rights reserved. Important Notices, Privacy Statement, and Trademarks of Cisco Systems, Inc.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0832
Fls:
Doc: 3701

Ap BU

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0833
Fls:
Doc: 3701

3194
21

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:

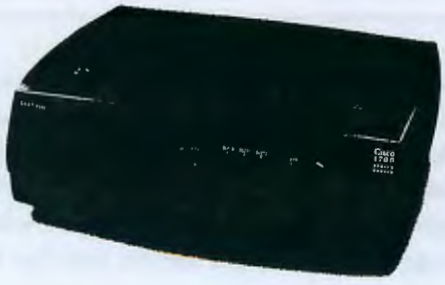
- Flexibility to adapt to changing requirements
- Modularity that allows you to individually configure the system to meet specific business needs
- Investment protection with features and performance to support new WAN services such as broadband DSL and cable access, multiservice voice/data integration, 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.

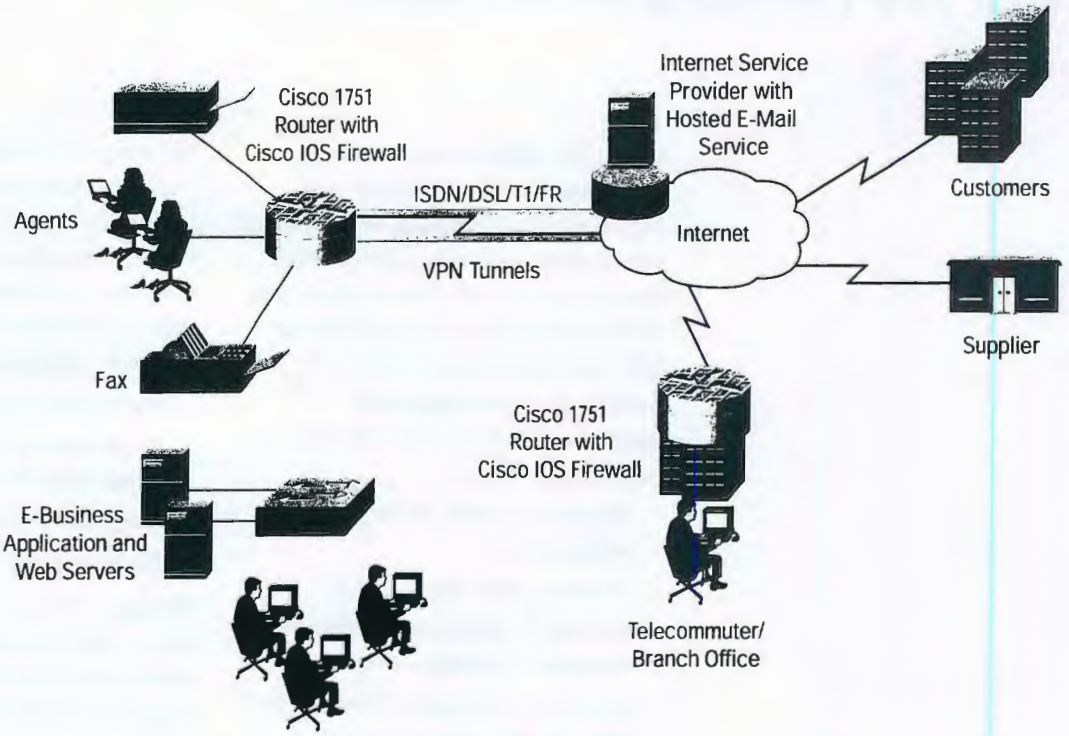
Figure 1
The Cisco 1751 Router delivers a versatile e-Business WAN access solution.



RQS Nº 03/2005 - CN
CPMI - CORREIOS
0834
Fls:
Doc: 3701

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

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.

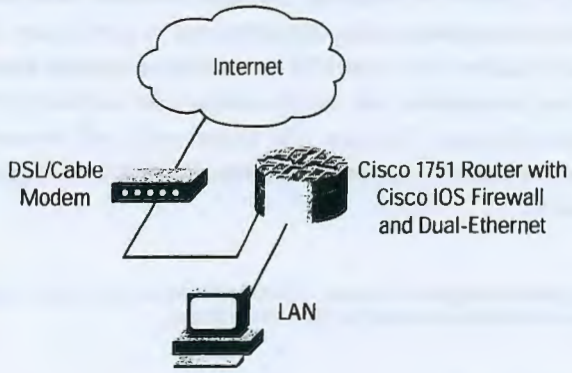
All Cisco 1751 models offer three modular slots for voice and data interface cards, an autosensing 10/100BaseT Fast Ethernet LAN port supporting standards-based IEEE 802.1Q VLAN, a console port, and an auxiliary port. The Cisco 1751 Router supports the same WAN interface cards as the Cisco 1600, 1700, 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,

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

3192
21

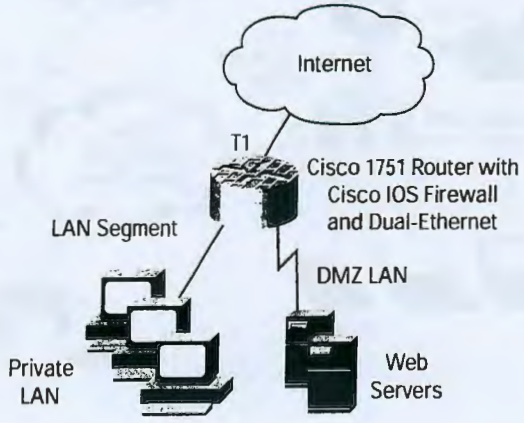
and serial with DSU/CSU options for primary and backup WAN connectivity. The voice interface cards support Foreign Exchange Office (FXO), Foreign Exchange Station (FXS), Network and User Side Voice BRI (ISDN BRI NT/TE), Ear & Mouth (E&M), direct inward dial (DID), and T1/E1 Multiflex VWICs. Additionally, 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.

POS Nº 03/2005 - CN
CPMI - CORREIOS
0835
Fls:
Doc: 3701

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Key Benefits

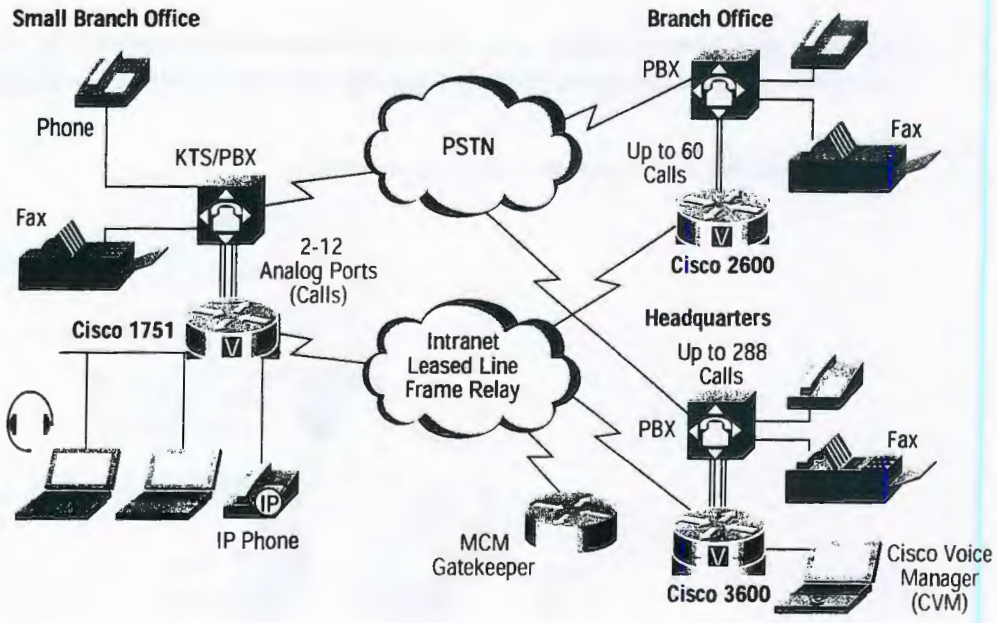
The Cisco 1700 Series routers support the value of end-to-end Cisco network solutions with the following benefits:

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

Cisco Systems, Inc.
All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

3190
21

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

RQS N° 03/2005 - CN
CPMI - CORREIOS
0836
Fls:
3701

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

3 189

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)

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

3188
21

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

ARQS Nº 03/2005 - CN
CPMI - CORREIOS
0837
Fls:
Doc: 3701

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

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 individually 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.

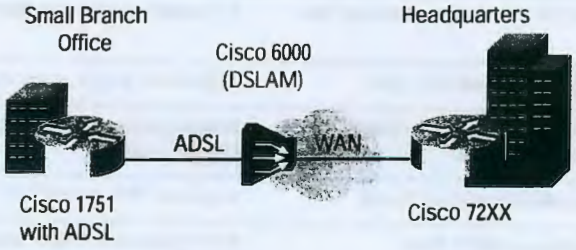
Because the Cisco 1751 Router provides robust voice compression, up to 8 voice calls can occupy a single 64K data channel simultaneously, without compromising data performance. Cisco IOS voice compression technology integrates data and voice traffic to enable efficient use of existing data networks.

Cisco Systems, Inc.
All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

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.

RQS Nº 03/2005 - CN - CORREIOS
Fls: 0838
Doc: 3701

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

3.185

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

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

3.184
2.

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

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0839
Fls:
Doc: 3701

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

3183

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

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

3.182
2

- 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.

RQS Nº 03/2005 - CN
CPMI - CORREIOS

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])

Doc: 3701

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

3.181
2

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 Mulitcast, Frame Relay SVC, RSVP, the NetWare Link Services Protocol (NLSP), AppleTalk SMRP, the Web Cache Control Protocol (WCCP), and the Network Timing Protocol (NTP).

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

3.180
2

- 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.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0841
Fls:
3701
Doc:

Cisco Systems, Inc.
All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

3.179
L

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=

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

3.178
2.

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

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0842
Fls:
Doc: 3701

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

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

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

- 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.

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

All contents are Copyright © 1992–2003, Cisco Systems, Inc. All rights reserved. Cisco, Cisco IOS, Cisco Systems, and the Cisco Systems logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0203R)

ETMG 202903_01/03

RQS Nº 03/2005 - CN - CPMI - CORREIOS
0184
Fls:
3791
Doc:

DOC.
000233

CPL/AC

PREGÃO
050/2003

LOCAÇÃO DE EQUIPAMENTOS DE INFORMÁTICA INCLUINDO ASSISTÊNCIA TÉCNICA E TREINAMENTO

HP INVENT – MANUAL APÊNDICES BV A CV

2003
PASTA 07

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 0844
Doc: 3701

ROS Nº 03/2005 CN
CPMI - CORREIOS
0845
Fls: 3701
Doc:

Apêndice BV

Close Window

Toolkit: Roll over tools t

Feedback | Help

ECT 14.703 1 CPL-AC

Cisco Systems

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	2600
Releases	12.2(15)T
Feature Set	IP PLUS

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
c2600-is-mz.12.2-15.T	64	32	S26CP-12215T= S26CP-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
AAA-PPP-VPDN Non-Blocking
Accounting of VPDN Disconnect Cause
ACL Authentication of Incoming RSH and RCP
ACL Sequence Numbering
Adaptive Frame Relay Traffic Shaping for Interface Congestion
Additional Vendor-Proprietary RADIUS Attributes
Address Resolution Protocol (ARP)
ADSL - Asymmetric Digital Subscriber Line Support
Advanced Voice Busyout (AVBO)
A oice-30, AIM-ATM-Voice-30
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 Call Queueing by Role
Asynchronous Line Monitoring
Asynchronous Rotary Line Queuing
Asynchronous Serial Traffic Over UDP
ATM Cell Loss Priority (CLP) Setting
ATM Multilink PPP Support on Multiple VCs
ATM Software Segmentation and Reassembly (SAR)
ATM Subinterface MIB/Traps
ATM SVC Troubleshooting Enhancements
ATM-DXI
Auditing Raw Buffers on a Channel Associated Signaling Interface
AutoInstall Using DHCP for LAN Interfaces
Automatic modem configuration
AutoQoS - VoIP
Bandwidth Allocation Control Protocol (BACP)

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0846
Fls: 3701
Doc:

4.702

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 Increased Support of Numbered as-path Access Lists
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 Route-Map Policy List Support
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
Call Release Source Reporting in Gateway-Generated Accounting Records
Call Status Tracking Optimization
er 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
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 Discovery Protocol (CDP) over ATM
Cisco IOS Telephony Service (ITS) Version 2.0
Cisco IOS Telephony Service (ITS) Version 2.01
Cisco IOS Telephony Service (ITS) Version 2.1
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
Class-Based RTP & TCP Header Compression
Classless InterDomain Routing (CIDR) IP Default Gateway
r Channel T3/E3 with Integrated CSU/DSU
CLI String Search
ClickStart
CNS Configuration Agent
CNS Event Agent
CNS Flow-Through Provisioning
Commented IP Access List Entries
Committed Access Rate (CAR)
Compression Control Protocol
Conferencing and Transcoding for Voice Gateway Routers
Configurable per ATM-VC Hold Queue size
Configurable Timers in H.225
Contact Closure Network Module
Content Engine Network Module for Caching and Content Delivery
Control Plane DSCP Support for RSVP
COPS for RSVP
CT1/RBS (Robbed Bit Signaling)
CUG Selection Facility Suppress Option
Custom Queueing (CQ)
Customer Profile Idle Timer Enhancements for Interesting Traffic
Default Passive Interface

RQS Nº 03/2005 - CN -
CPMI - CORREIOS
0847
Fls:
3701
Doc:

ECT 4.701 CPI-A2

Default VPDN Group Template
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 - MPLS VPN Support
DHCP Relay Agent Support for Unnumbered Interfaces
DHCP Secured IP Address Assignment
DHCP Server - On Demand Address Pool Manager
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
Diffserv Compliant WRED
Digital J1 Voice Support
D[illegible] Inward Dial (DID)
DLSw Enhancements: PGM RFC-3208 Compliance
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
DTMF Relay for SIP Calls Using Named Telephone Events (NTE)
D[illegible]nic Multiple Encapsulation for Dial-in over ISDN
ETR2 Signaling
Easy IP (Phase 1)
EIGRP Nonstop Forwarding (NSF) Awareness
Encrypted Vendor Specific Attributes
Enhanced Call and IVR Control for Rotary Call Set Ups
Enhanced Codec support for SIP using Dynamic Payloads
Enhanced Debug Capabilities for Cisco Voice Gateways
Enhanced G.168 Echo Cancellation
Enhanced IGRP (EIGRP)
Enhanced IGRP Stub Routing
Enhanced ITU-T G.168 Echo Cancellation
Enhanced Local Management Interface (ELMI)
Enhanced Packet Marking
Enhanced Password Security
Enhanced Tracking Support.
Express RTP and TCP Header Compression
Fast Fragmentation (Fast-Switched Fragmented IP Packets)
Fast-Switched Compressed RTP
Fast-Switched Policy Routing
Fast-Switched SRTLB

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0848
Fls: 3701
Doc:

Feature Group D Support
Flow-Based WRED
Forced Calling Line Identifier
Frame Relay
Frame Relay - Multilink (MLFR-FRF.16)
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 PVC Bundles with IP QoS Support
Frame Relay PVC Bundles with MPLS QoS Support
Frame Relay PVC Interface Priority Queueing
Frame Relay Queuing and Fragmentation at the Interface
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)
ne Relay Tunnel Switching
me Relay Voice Adaptive Traffic Shaping
FXO Answer and Disconnect Supervision
G.SHDSL Symmetric DSL Support
Gatekeeper Ecosystem Interoperability
Gateway Enhancements to Enable v4-v2 Interworking
Gateway Support for Advanced Busy Out for Gatekeeper Registration
Generic Routing Encapsulation (GRE)
Generic Routing Encapsulation (GRE) Tunnel Keepalive
Generic Traffic Shaping (GTS)
GLBP: Gateway Load Balancing Protocol
Globalized Cadence and Tone for Cisco IOS Gateways
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
H.323v4 - Enhanced Call Usage Reporting
H.323V4 Gateway Zone Prefix Registration Enhancements
H450.2 & H450.3 Support In IOS
Half bridge/half router for CPP and PPP
Hoot and Holler over IP
HSRP - Hot Standby Router Protocol
P over ISL
RP support for ICMP Redirects
HTTP 1.1 Web Server
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
Integrated routing and bridging (IRB)
Inter-Domain Gateway Security Enhancement
Interface Alias Long Name Support
Interface Index Display
Interface Index Persistence
Interface Range Specification
Internal Cause Code Consistency between SIP and H.323

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0849
Fls:
Doc: 3701

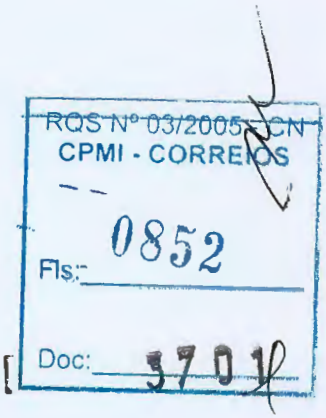
Inverse Multiplexing over ATM (IMA)
IP DSCP marking for Frame-Relay PVC
IP Enhanced IGRP Route Authentication
IP Header Compression Enhancement - PPPoATM and PPPoFR Support
IP Multicast Load Splitting across Equal-Cost Paths
IP Named Access Control List
IP Precedence for GRE Tunnels
IP Routing
IP RTP Priority
IP Summary Address for RIPv2
IP-to-ATM CoS
IPSec Through Network Address Translation Support
IPv6 ADSL and Dial Deployment Support
IPv6 Extended Access Control List
IPv6 for Cisco IOS Software
IPv6 ISATAP Tunnel Support
IPv6 Quality of Service
ISDN
ISDN Advice of Charge (AOC)
ISDN Caller ID Callback
ISDN Cause Code Override
ISDN Generic Transparency Descriptor (GTD) for Setup Message
ISDN Leased Line at 128kbps
ISDN Network Side for ETSI Net5 PRI
ISDN NFAS
ISDN Progress Indicator support for SIP using 183 Session Progress
I[illegible]'LAN
IV[illegible] Enhanced Multilanguage Support
L2TP Dial-Out
L2TP Extended Failover
L2TP Layer 2 Tunneling Protocol
L2TP Tunnel Preservation of IP TOS
LAN Network Manager over DLSw+
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 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
Malicious Caller Identification (MCID) Invocation Support for Enterprise Ne...
MD5 File Validation
Measurement-Based Call Admission Control for SIP
Message Banners for AAA Authentication
MGCP - Media Gateway Control Protocol
M[illegible]P 1.0 Including NCS 1.0 and TGCP 1.0 Profiles
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 support for CallManager (IP-PBX)
MGCP VoIP Call Admission Control
Microsoft Point-to-Point Compression (MPPC)
Mobile IP
Mobile IP - Challenge/Response Extestions
Mobile IP - Dynamic DNS and Multiple DHCP Support
Mobile IP - Fastswitching Support on FA
Mobile IP - Generic NAI Support and Home Address Allocation
Mobile IP - HA Accounting
Mobile IP - HA Policy Routing
Mobile IP - HMAC-MD5 support
Mobile IP - IPSec for HA-FA Tunnel
Mobile IP - Mobile Networks
Mobile IP - Mobile Networks Asymmetric Link and Dynamic Network
Mobile IP - Mobile Networks Priority HA Assignment

ECT 4.699 J CPL-M
RQS Nº 03/2005 - CN
CPMI - CORREIOS
0850
Fls:
3701
Doc:

Mobile IP - Mobile Networks Static Collocated Care of Address
Mobile IP - Mobile Networks Tunnel Templates for Multicast
Mobile IP - NAT Detect
Mobile IP - Private Addressing Support
Mobile IP - Proxy Mobile IP and Proxy CHAP
Mobile IP - Single IDB Tunnel Support
Mobile IP - Support for FA Reverse Tunnelling
Mobile IP - Support NAI Based MNs that are serviced by many HAs
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)
Modular QoS CLI (MQC) - Based Frame Relay Traffic Shaping
Modular QoS CLI (MQC) Three-Level Hierarchical Policer
Modular QoS CLI (MQC) Unconditional Packet Discard
MS Callback
MS-CHAP Version 1
MS-CHAP Version 2
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)
Multiclass Multilink PPP
Multihop VPDN
Multilink PPP
Named Method Lists for AAA Authorization and Accounting
NAT - Static Mapping Support with HSRP for High-Availability
NAT Default Inside Server Enhancement
NAT Integration with MPLS VPNs
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
On Demand Routing (ODR)
Optimized PPP Negotiation
OSPF
OSPF ABR type 3 LSA Filtering
OSPF Flooding Reduction
OSPF for IPv6
OSPF Forwarding Address Suppression in Translated Type-5 LSAs
OSPF Inbound Filtering using Route Maps with a Distribute List
OSPF Nonstop Forwarding Awareness
OSPF Not-So-Stubby Areas (NSSA)
OSPF On Demand Circuit (RFC 1793)

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0851
Fls:
Doc: 3701

OSPF Packet Pacing
OSPF Sham-Link Support for MPLS VPN
OSPF Shortest Paths First Throttling
OSPF Stub Router Advertisement
OSPF Support for Fast Hellos
OSPF Support for Multi-VRF on CE Routers
OSPF Update Packet-Pacing Configurable Timers
Packet Classification Based on Layer3 Packet-Length
Packet Classification using Frame-Relay DLCI Number
PAD Subaddressing
Parse Bookmarks
Parser Cache
Password Authentication Protocol (PAP)
Per-User Configuration
Percentage-Based Policing and Shaping
PIM Dense Mode State Refresh
PIM MIB Extension for IP Multicast
PIM Version 1
PIM Version 2
Policer Enhancement - Multiple Actions
Policy-Based Routing (PBR)
PPP
PPP over ATM
PPP Over Fast Ethernet 802.1Q
PPP over Frame Relay
PPPoE Client
P[illegible].931 Signaling Backhaul for Call Agent Applications
P[illegible]ty Queueing (PQ)
Privilege Command Enhancement
PSTN Fallback
QoS Device Manager (QDM)
QoS for Virtual Private Networks
QoS Packet Marking
QoS Priority Percentage CLI Support
QSIG Backhaul (TCP based) for Cisco IOS Gateways
QSIG Protocol Support
Qualified Logical Link Control (QLLC)
RADIUS
RADIUS Attribute 44 (Accounting Session ID) in Access Requests
RADIUS Attribute 82: Tunnel Assignment Id
RADIUS Centralized Filter Management
RADIUS EAP Support
RADIUS for Multiple User Datagram Protocol Ports
RADIUS Interim Update at Call Connect
RADIUS Route Download
RADIUS Tunnel Preference for Load Balancing and Fail-over
Random Early Detection (RED)
Redial Enhancements
Reflexive Access Lists
R[illegible]onse Time Reporter (RTR)
Response Time Reporter (RTR) enhancements
Reverse Path Forwarding - Source Exists only
RGMP - Router-Port Group Management Protocol
RIP
RMON events and alarms
Rotating Through Dial Strings
RSVP - Resource Reservation Protocol
RSVP Local Policy Support
RSVP Message Authentication
RSVP Refresh Reduction and Reliable Messaging
RSVP Scalability Enhancements
RSVP Support for Frame Relay
RSVP support for LLQ
RSVP Support for RTP Header Compression
RTP Header Compression
SDLC SNRM Timer and Window Size Enhancements
SDLC-to-LAN conversion (SDLLC)
Selective Packet Discard (SPD)
Selective Virtual-Access Interface Creation
Service Assurance Agent (SAA) APM Application Performance Monitor



Service Assurance Agent (SAA) DHCP Operation
Service Assurance Agent (SAA) DLSW Operation
Service Assurance Agent (SAA) DNS Operation
Service Assurance Agent (SAA) for ATM Interfaces
Service Assurance Agent (SAA) Frame Relay Operation
Service Assurance Agent (SAA) FTP Operation
Service Assurance Agent (SAA) HTTP 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) SNMP Support
Session Limit Per VRF
SGCP RSIP and AUEP Enhancements
Shell-Based Authentication of VPDN Users
Show Command Redirect
Single Rate 3-Color Marker for Traffic Policing
SIP - Call Transfer Enhancements Using Refer Method
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 and H.323 Fax Enhancements
SIP Carrier Identification Code
Diversion Header Implementation for Redirecting Number
Enhanced 180 Provisional Response Handling
SIP Extensions for Caller Identity and Privacy
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 Redirect Processing Enhancement
SIP Session Timer Support
SIP Support for Media Forking
SIP T.37 and Cisco Fax
SIP T.38 Fax Relay
SIP Transfer Using the Refer Method and Call Forwarding
SIP: Core SIP Technology Enhancements
SIP: ISDN Suspend/Resume Support
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
MP 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 1.0
SRST: Survivable Remote Site Telephony Version 2.0
SRST: Survivable Remote Site Telephony Version 2.02
SRST: Survivable Remote Site Telephony Version 2.1
Stack Group Bidding Protocol (SGBP)
Standard IP Access List Logging
Static Cache Entry for IPv6 Neighbor Discovery
Stub IP Multicast Routing
STUN (Serial Tunnel)

4.696
RQS Nº 03/2005 - CN
CPMI - CORREIOS
0853
Fls:
Doc: 3701

Subnetwork Bandwidth Manager (SBM)
Subscriber Service Switch
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.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
Traffic Policing
Transmit Ring Tuning Enhancements
Transparent Bridging
Transparent CCS and Frame Forwarding Enhancements
Transparent Common Channel Signaling (T-CCS)
Trunk Conditioning for FRF.11 and Cisco Trunks
Tunnel Type of Service (TOS)
Tunneling of Asynchronous Security Protocols
Turbo Flooding of UDP Datagrams
T[illegible]Rate Policer
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)
Unspecified Bit Rate Plus (uBR+) and ATM Enhancements
User Maximum Links
Using 31-bit Prefixes on IPv4 Point-to-Point Links
V.120 Support
Virtual Interface Template Service
Virtual Private Dial-up Network (VPDN)
Virtual Profile CEF Switched
Virtual Profiles
Virtual Router Redundancy Protocol (VRRP)
Voice Busyout Enhancements
Voice Call Tuning
Voice DSP Control Message Logger
Voice over Frame Relay (FRF.11)
Voice over Frame Relay Configuration Updates
Voice Over IP
VoiceXML Voice Store and Forward
VoIP and Cisco Express Forwarding (CEF) Interoperability
VoIP and Policy Based Routing (PBR) Interoperability
V[illegible]Call Admission Control using RSVP
VoIP Gateway Trunk and Carrier Based Routing Enhancements
VoIP Outgoing Trunk Group Identification and Carrier ID for Gateways
VoIP Trunk Group Label Routing Enhancement
VPDN Group Session Limiting
VPDN Multihop by DNIS
VPN Tunnel Management
WCCP Redirection on Inbound Interfaces
WCCP Version 1
WCCP Version 2
Weighted Fair Queueing (WFQ)
Weighted RED (WRED)
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 Closed User Group
X.25 Failover
X.25 Load Balancing
X.25 on ISDN D-Channel
X.25 over Frame Relay (Annex G)

4.695
RQS Nº 03/2005 - CN
CPMI - CORREIOS
0854
Fls:
3701
Doc:

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
XGCP Bind Command for Control and Media Packets

To find out more about your selected release, you can use the Bug Toolkit

Close Window

© 1992-2003 Cisco Systems, Inc. All rights reserved. Important Notices, Privacy Statement, and Trademarks of Cisco Systems, Inc.

Apêndice BX

ROS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 0856
Doc: 3701

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.

ECT 4.693 CPL-SG
DOS N° 03/2005 - CN
CPMI - [redacted] 1-1 DS
0857
Fls:
3701
Doc:

S.C.T. 4.692 CPMI

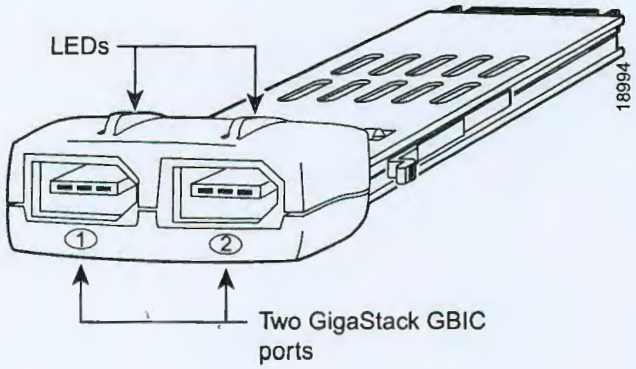
- Support for redundant loop configurations in a GigaStack GBIC stack

  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



RQS Nº 78/2003 - CN
CPMI - CORREIOS
0858
Fls:
3701
Doc:

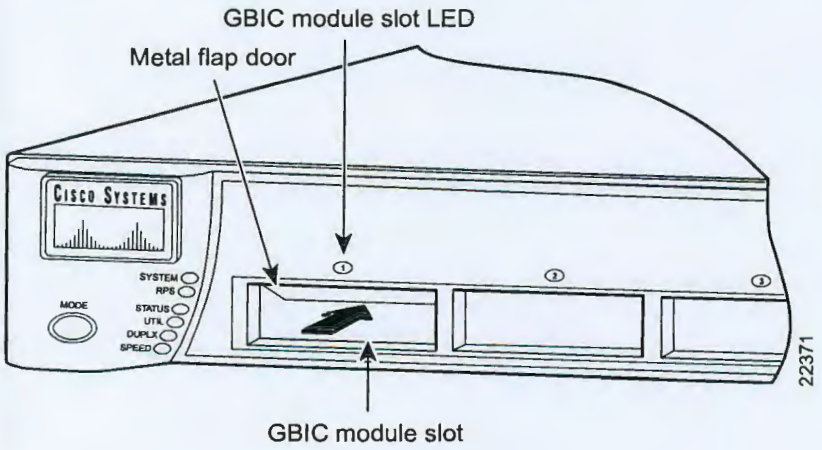
Table 1-1 GigaStack GBIC LEDs

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



RQS Nº 03/2005 - CN - CPMI - CORREIOS
Fls: 0859
Doc: 3701

Figure 1-3 GBIC LED Location on a 1000BASE-X Module

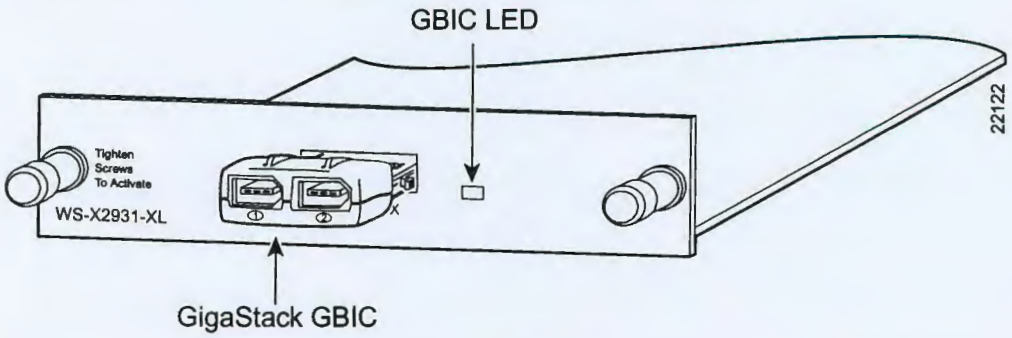


Table 1-2 describes the switch and 1000BASE-X module GBIC slot LED colors and port status.

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.

78-6460-04
CPMI - CORREIOS
Fls: 0860
Doc: 3701

4.689

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

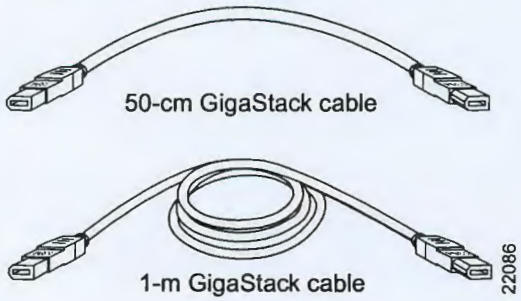


Table 1-3 GigaStack GBIC Cable Part Numbers

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.

RQS Nº CN
CPMI - CORREIOS
0861
Fls:
3701
Doc:

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

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0862
Fls:
3701
Doc:

4.687
J

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.

RQS N 03/2005 - CN -
CPMI - CORREIOS
0863
Fls:
3701
Doc:

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.

78-6460-04
RQS N° 03/2005 - CN
CPMI - CORREIOS
Fls: 0864
3701
Doc:

ECT 4.685 J

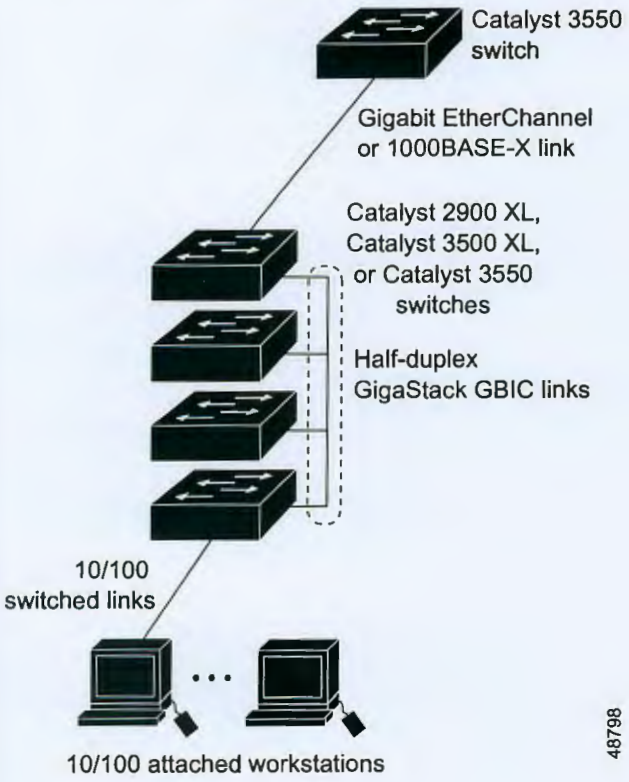
Deployment Examples

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



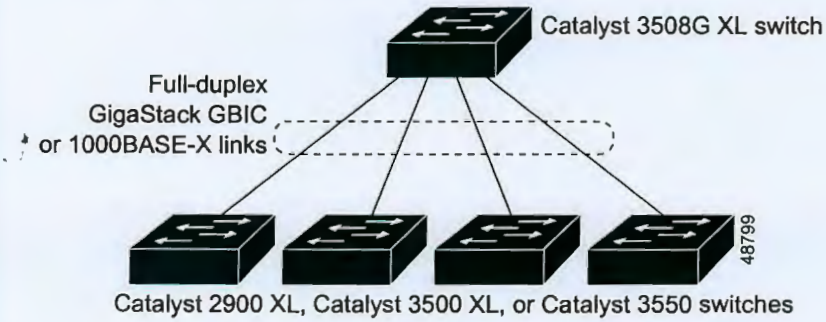
ROS Nº 03/2005 - CN
CPMI - CORREIOS
0865
Fls:
3701
Doc:

4.684
J

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



78-6460-04
RQS 05/2005 - CN
CPMI - CORREIOS
0866
Fls:
3701
Doc:

Apêndice BZ

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0867
Fls:
3701
Doc:

4.683
CPL-AC

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, page 3-2
- Verifying Switch Operation, page 3-10
- Installing the Switch in a Rack, page 3-10
- Installing the Switch on a Table, Shelf, or Desk, page 3-22
- Installing the Switch on a Wall, page 3-23
- Installing the GBIC Modules, page 3-26
- Installing and Removing SFP Modules, page 3-28
- Connecting to 10/100 and 10/100/1000 Ports, page 3-32
- Connecting to 100BASE-FX and 1000BASE-SX Ports, page 3-36
- Connecting to an LRE Port, page 3-38
- Connecting to GBIC Module Ports, page 3-44
- Connecting to an SFP Module, page 3-49
- Where to Go Next, page 3-50

RQS Nº
CPMI - CORREIOS
0868
Fls:
3701
Doc:

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, "Translated 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.**

4.681

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.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0869
Fls:
3701
Doc:

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.

4.679
1

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

RQS Nº 03 3-5
CPMI - CORREIOS
Fls: 0870
Doc: 3701

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 기기이
오니 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) megfeleloen 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.**

4.677
3

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.

ROS - CN
CPMI - CORREIOS
0871
Fls: 3701
Doc:

- 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

4.675

  - 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.

CPMI 3-9
0872
Fls: 3701
Doc:

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

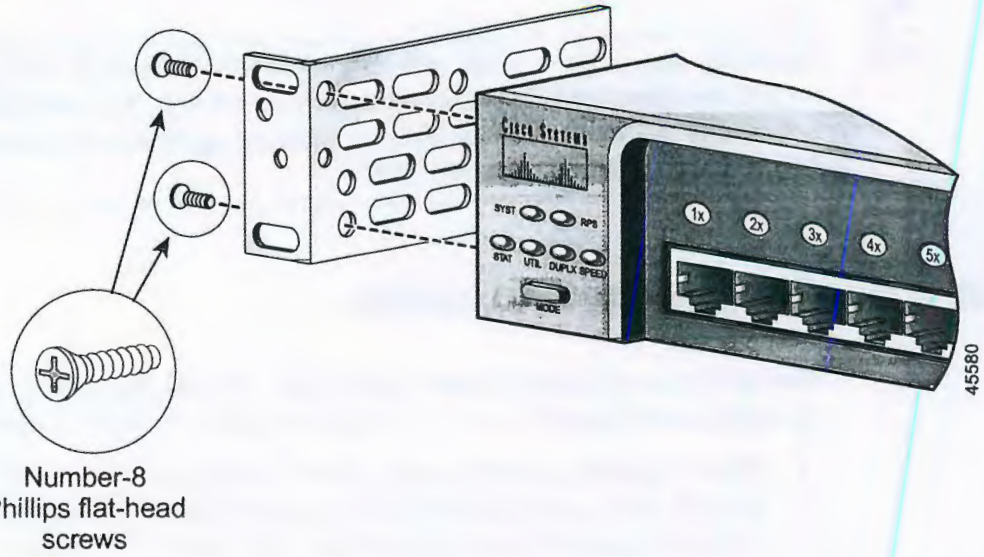
The bracket orientation and the screws that you use depend on whether you are attaching the brackets to a 19-, 23-, or 24-inch rack. Follow these guidelines:

- 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.

4.6
CPMI - CORREIOS
0873

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)



4.671

Figure 3-2 Attaching Brackets on the Switch in a 19-Inch Rack (Rear Panel Forward)

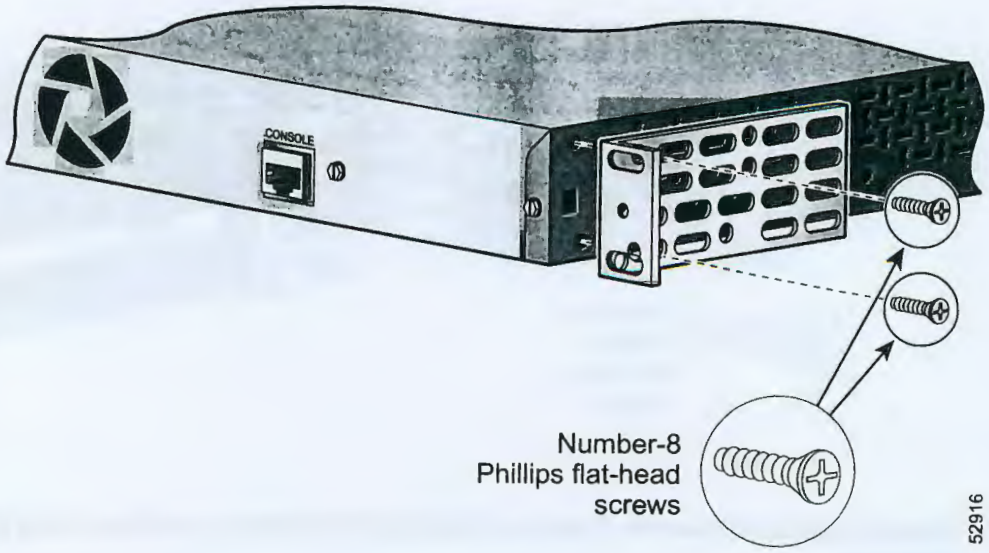
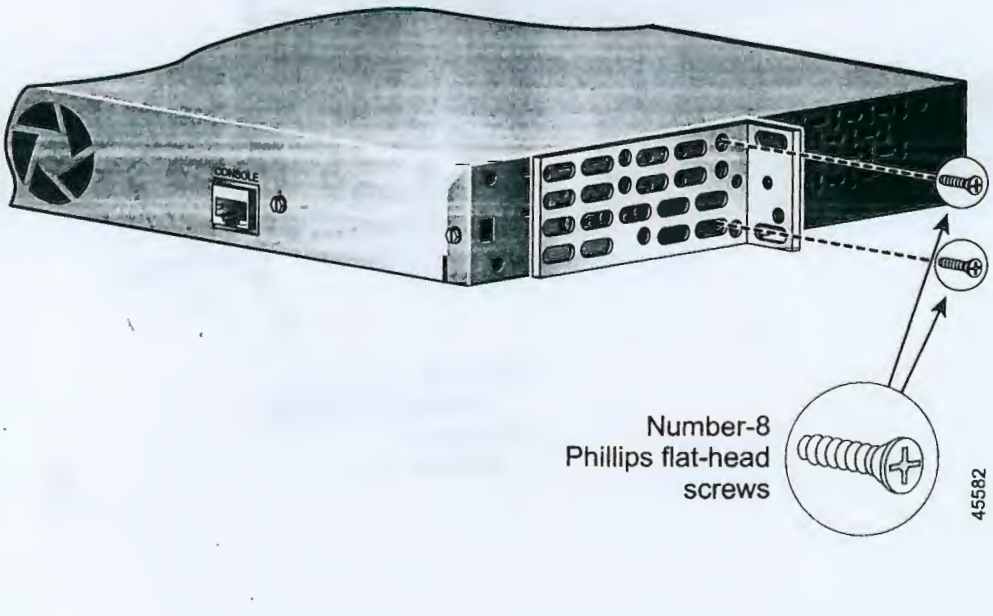


Figure 3-3 Attaching Brackets on the Switch in a 19-Inch Telco Rack



RQS N 3.13 - CN
CPMI - CORREIOS
Fls: 0874
Doc: 3701

Figure 3-4 Attaching Brackets on the Catalyst 2950G-48-EI Switch in a 19-Inch Rack (Front Panel Forward)

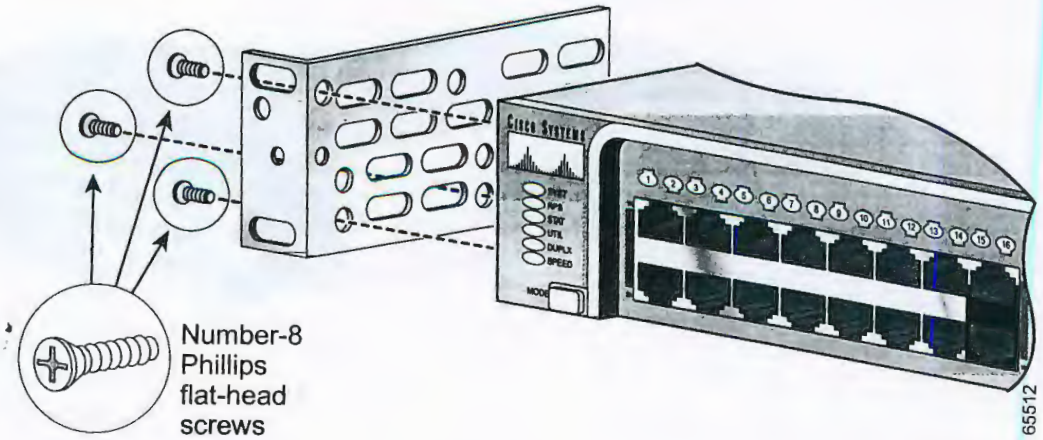
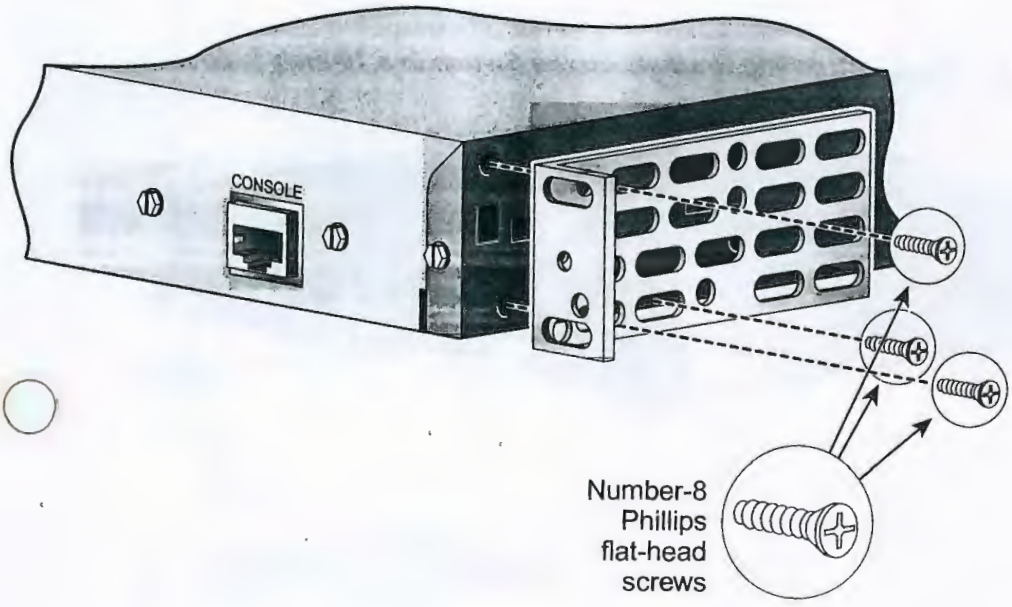


Figure 3-5 Attaching Brackets on the Catalyst 2950G-48-EI Switch in a 19-Inch Rack (Rear Panel Forward)



ECT 4.669 CPMI AC

Figure 3-6 Attaching Brackets on the Catalyst 2950G-48-EI Switch in a 19-Inch Telco Rack

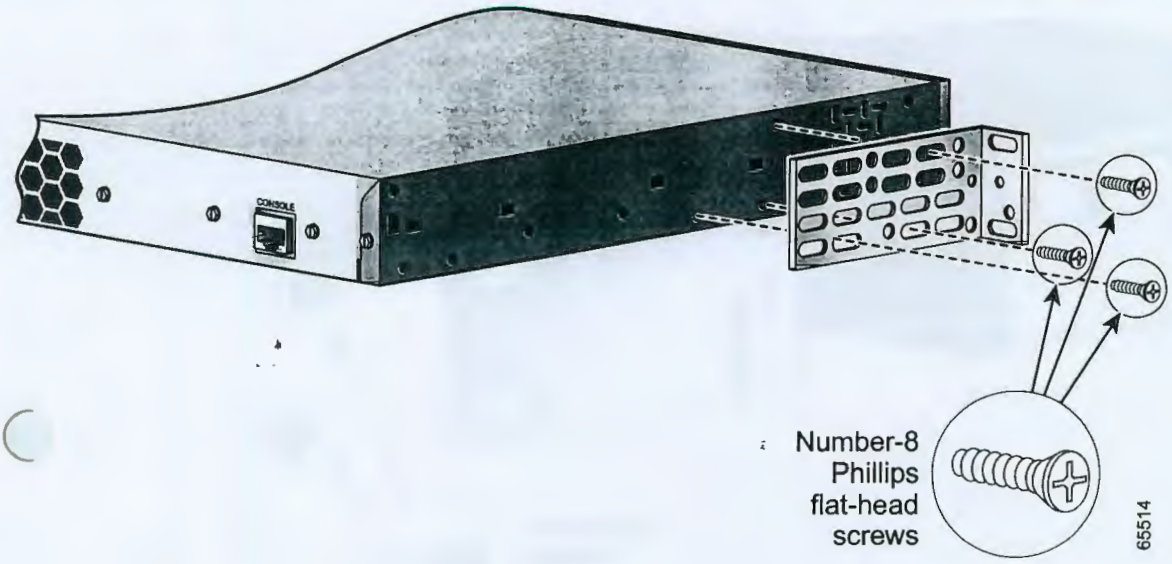
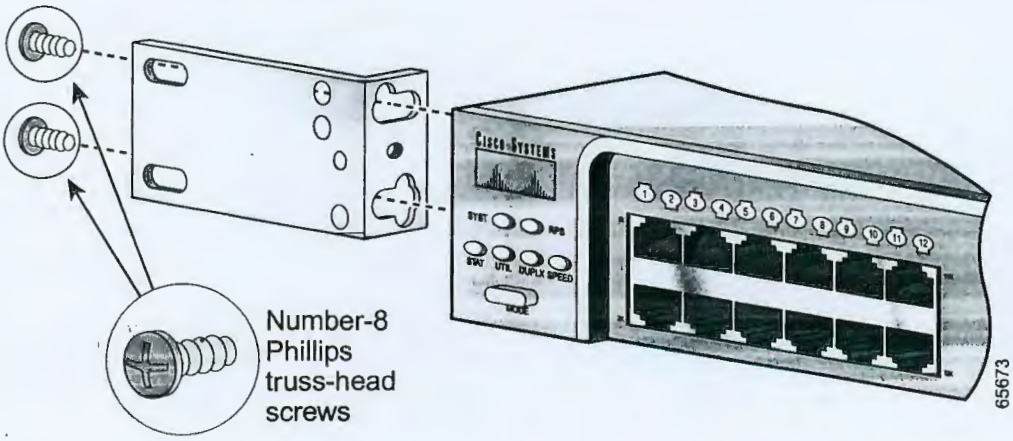


Figure 3-7 Attaching Brackets on the Catalyst 2950G-24-EI-DC or 2950ST-24 LRE 997 Switch in a 23-Inch Telco Rack (Front Panel Forward)



CPMI 3-15
0875
Fls:
3701
Doc:

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)

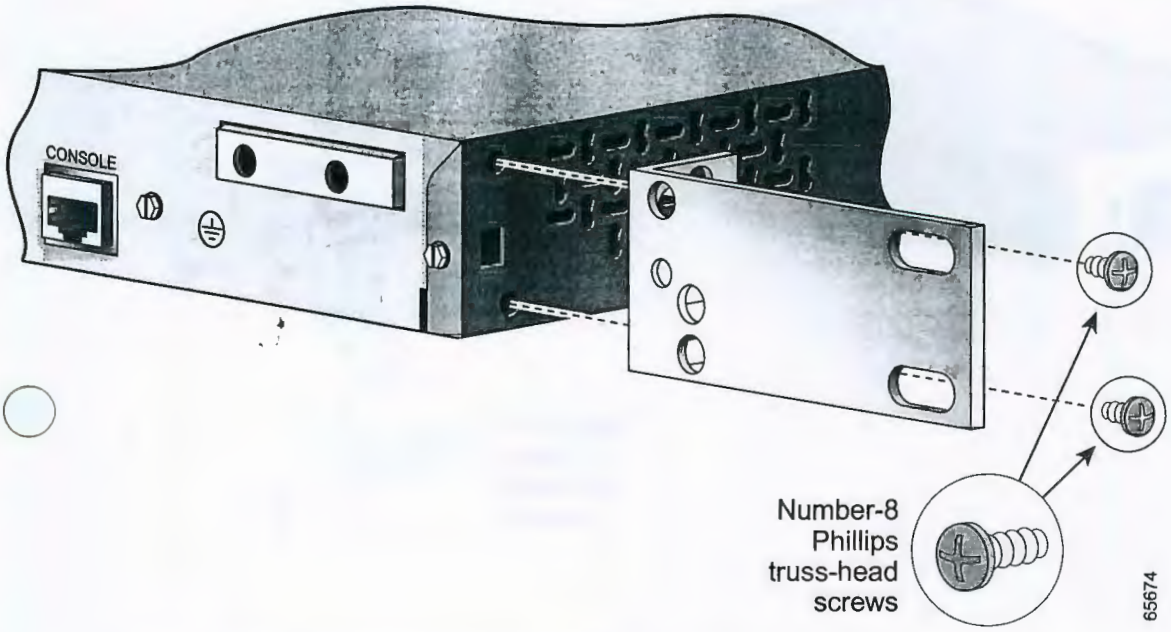


Figure 3-9 Attaching Brackets on the Catalyst 2950G-24-EI-DC or 2950ST-24 LRE 997 Switch in a 23-Inch Telco Rack

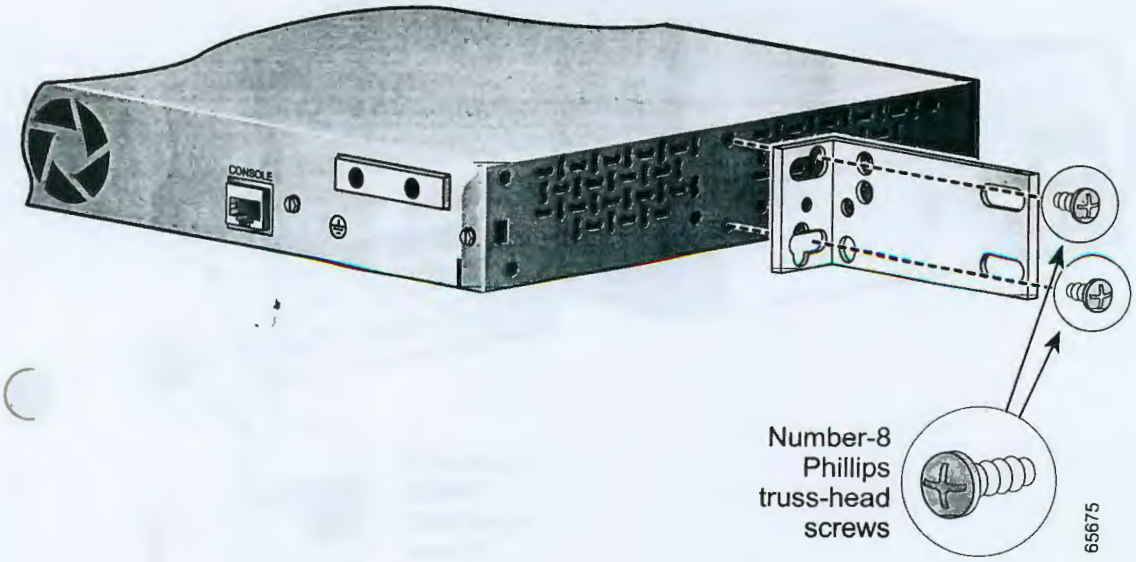


Figure 3-10 Attaching Brackets on the Switch in a 24-Inch Rack (Front Panel Forward)

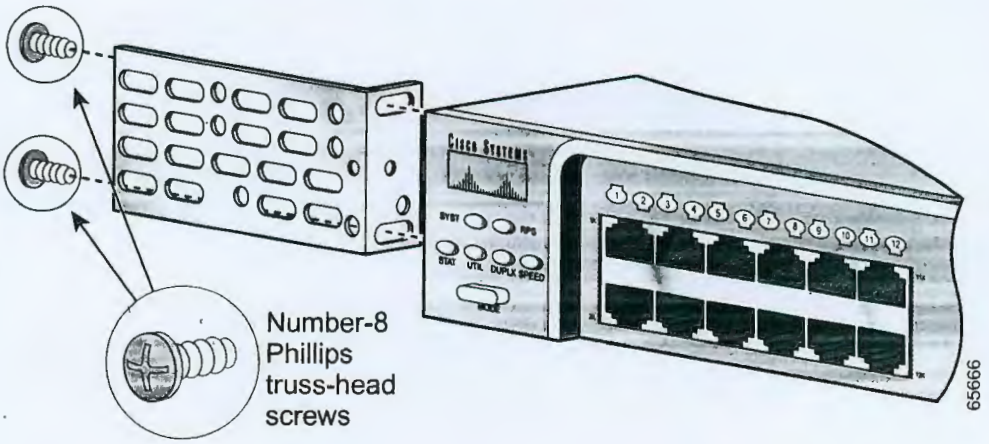
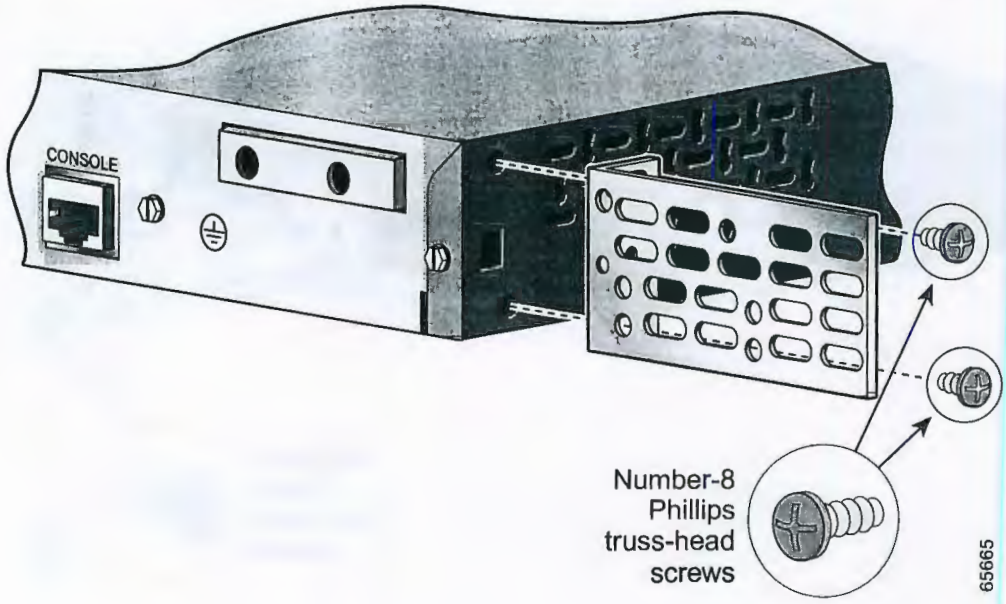


Figure 3-11 Attaching Brackets on the Switch in a 24-Inch Rack (Rear Panel Forward)



4.665
J

Figure 3-12 Attaching Brackets on the Switch in a 24-Inch Telco Rack

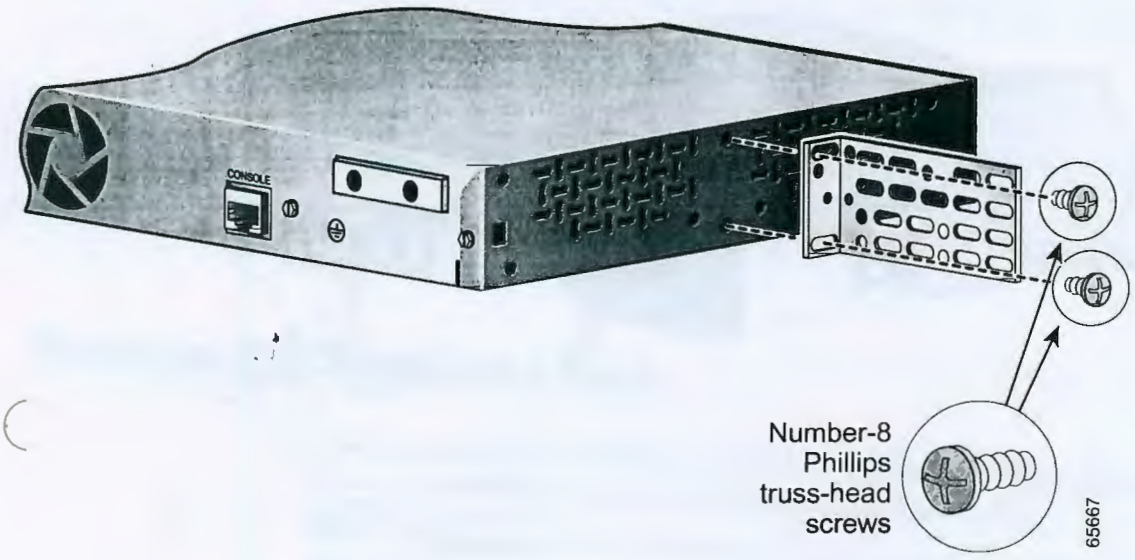
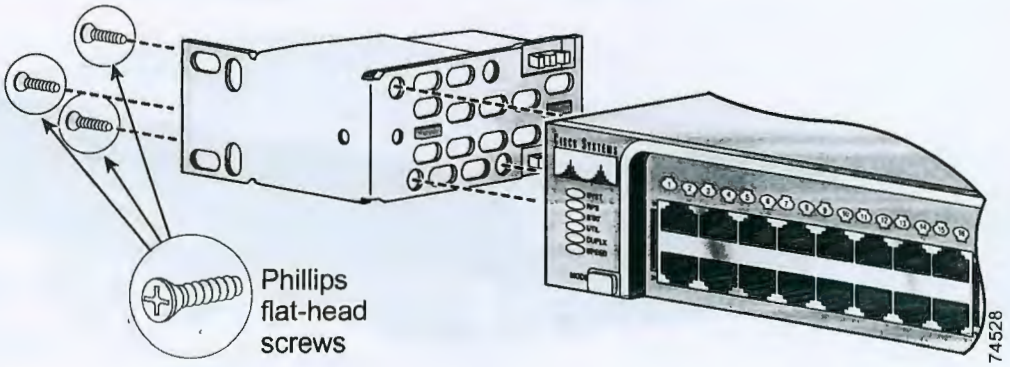


Figure 3-13 Attaching Brackets on the Catalyst 2950G-48-EI Switch in a 24-Inch Rack (Front Panel Forward)



RQS N - CN
CPMI - CORREIOS
0877
Fls:
3701
Doc:

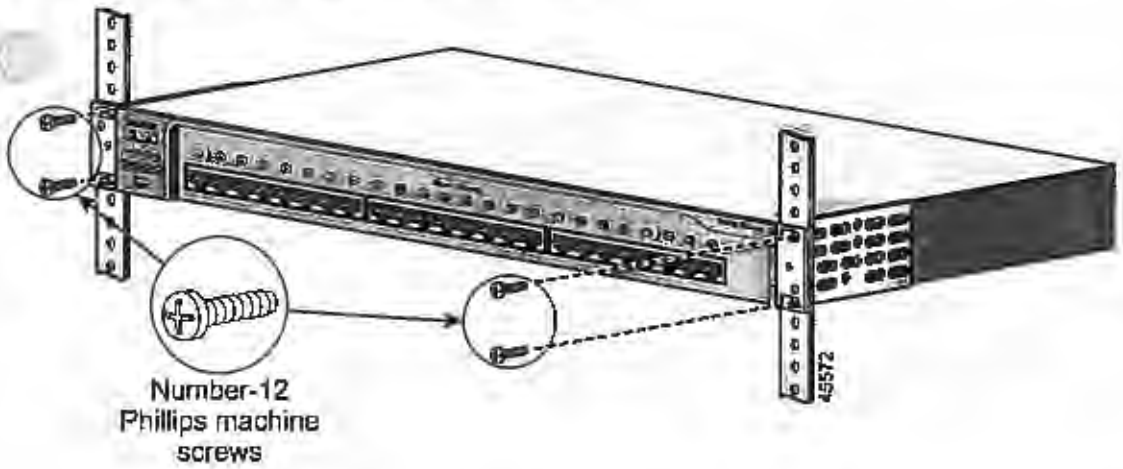
4.663
J

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.

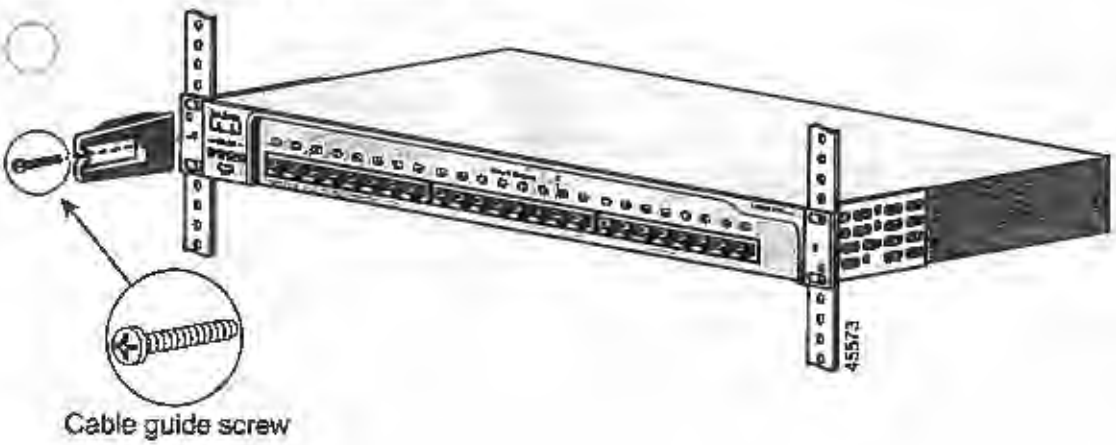
CP EIOS
Fls 0878
Doc 3701

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 with 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.

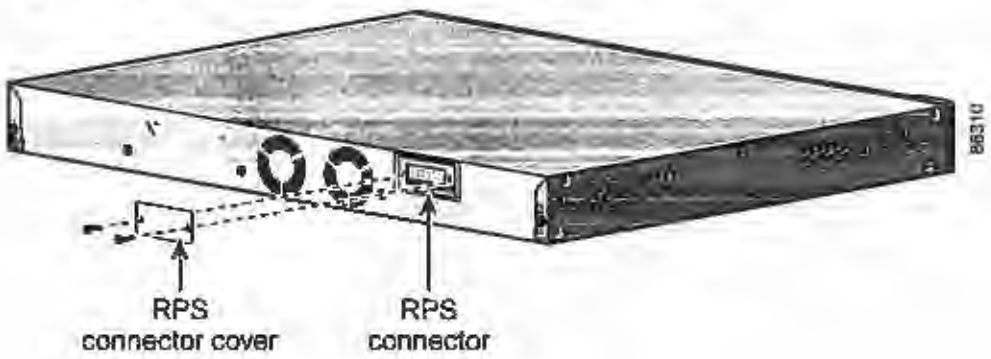
Figure 3-18 Attaching Brackets for Wall-Mounting for the Catalyst 2950 Switch

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

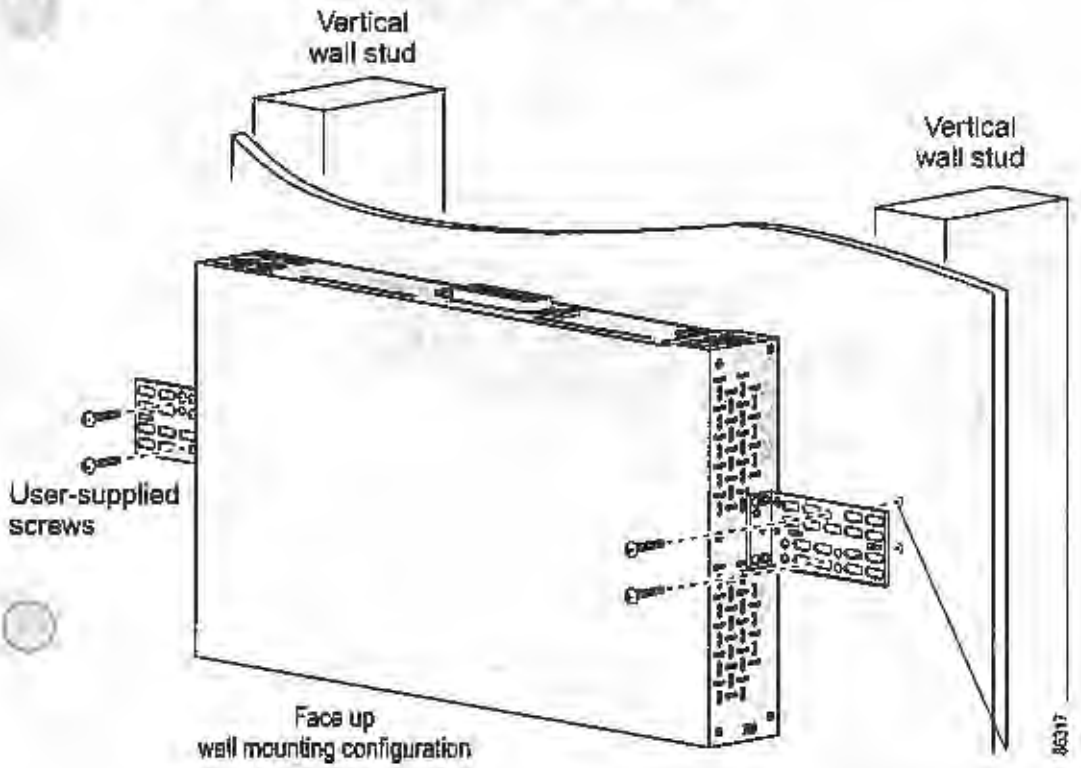


Mounting the Switch to a Wall

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

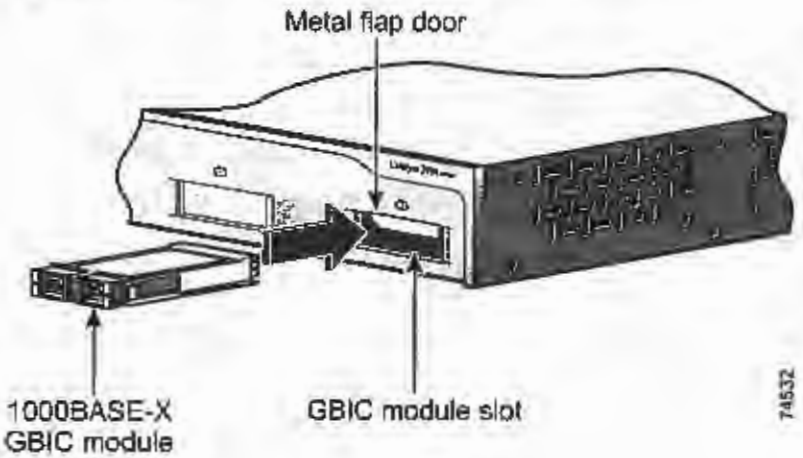


Figure 3-22 Installing a 1000BASE-T GBIC Module in a Switch

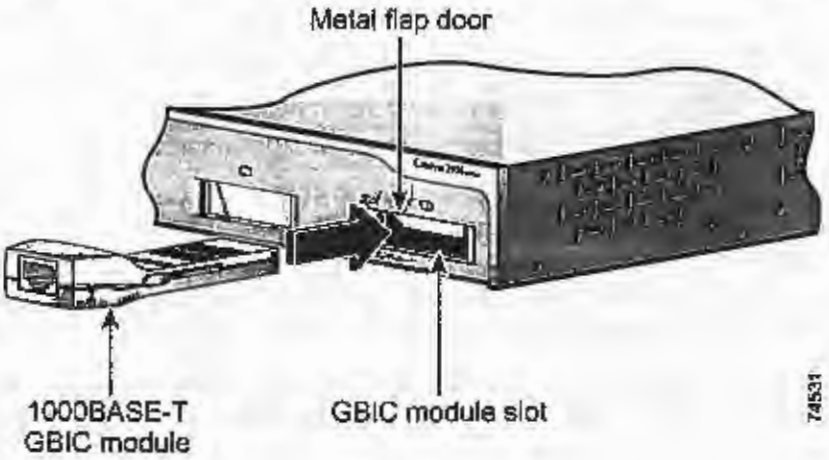
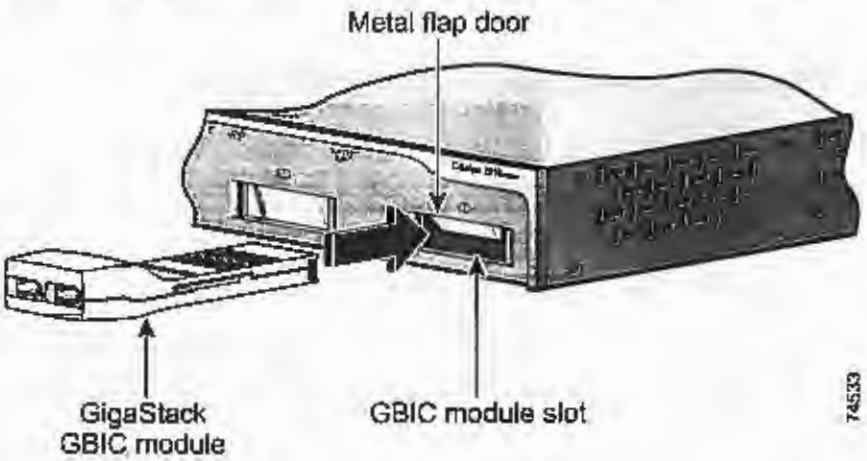


Figure 3-23 Installing a GigaStack GBIC Module in a Switch



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

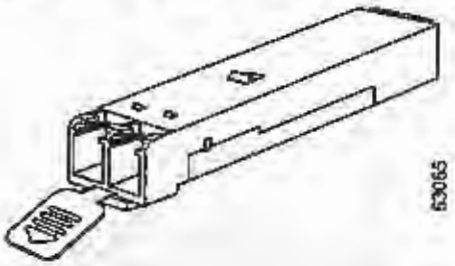


Figure 3-25 SFP Module with an Actuator Button Latch

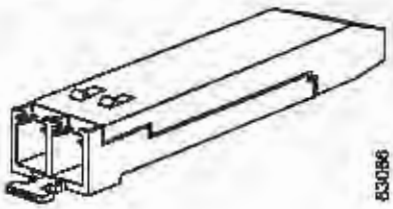
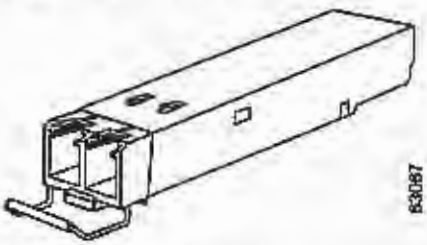


Figure 3-26 SFP Module with a Bale-Clasp Latch



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.

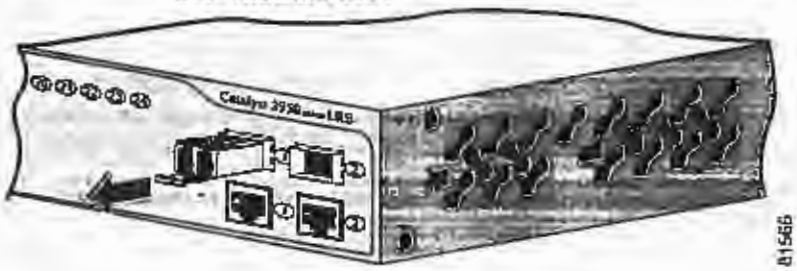
Step 4 Unlock and remove the SFP module, as shown in Figure 3-28, Figure 3-29, and Figure 3-30.

- 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

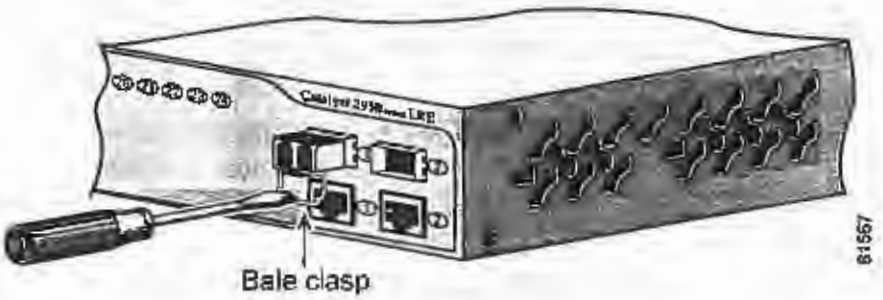
- If the module has an actuator button latch, use your thumb to push inward on the wedge to free the locking pin, and use your index finger to grip the ridge on top of the SFP module. Pull straight out to remove the module.

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.

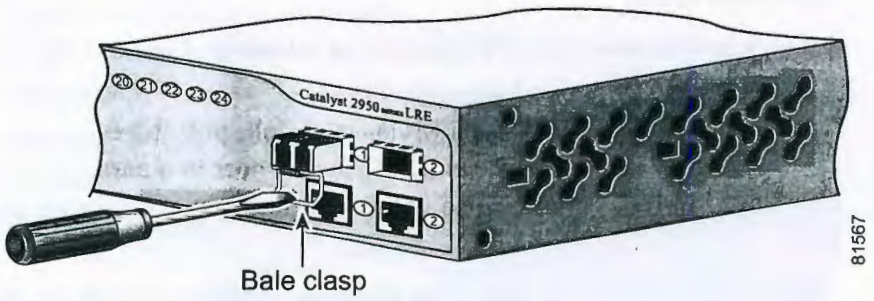
Connecting to 10/100 and 10/100/1000 Ports

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.

Figure 3-14 Attaching Brackets on the Catalyst 2950G-48-EI Switch in a 24-Inch Rack (Rear Panel Forward)

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.

4.651
CPI - AC

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.

RGS - CN
CPMI - CORREIOS
Fls: 0884
3701
Doc:

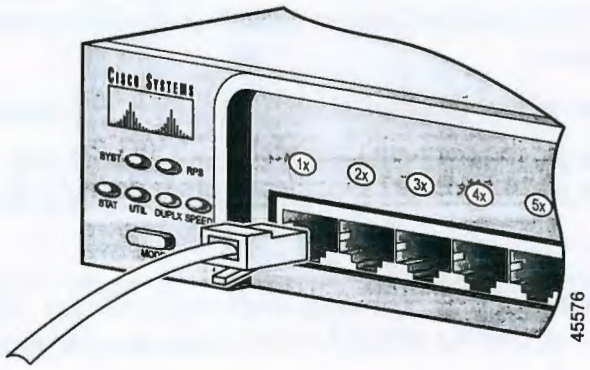
Follow these steps to connect the switch to 10BASE-T, 100BASE-TX, or 1000BASE-T devices:

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



4.649
J

Figure 3-32 Connecting to a Port on Catalyst 2950G-12-EI, 2950G-24-EI, and 2950G-24-EI-DC Switches

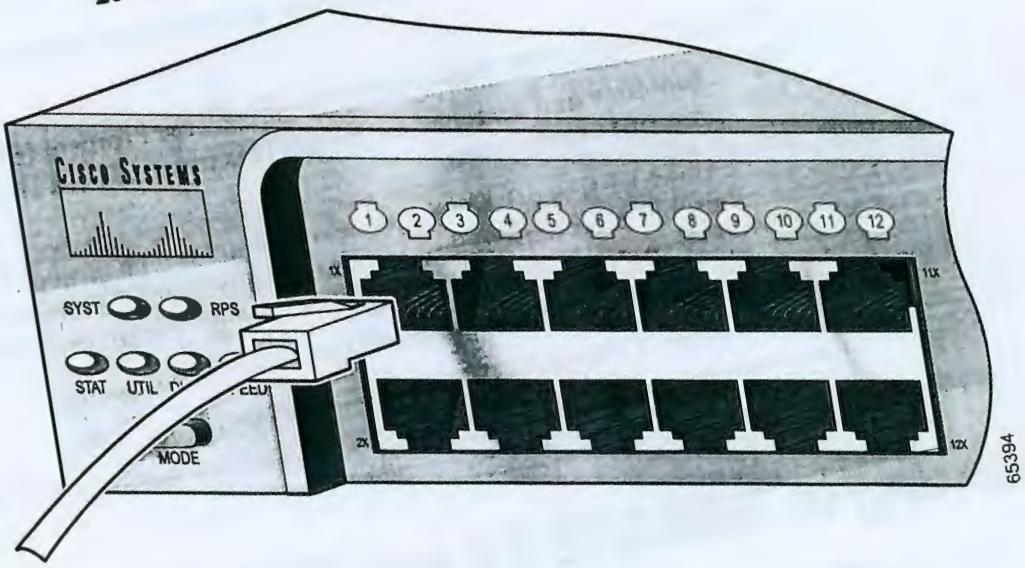
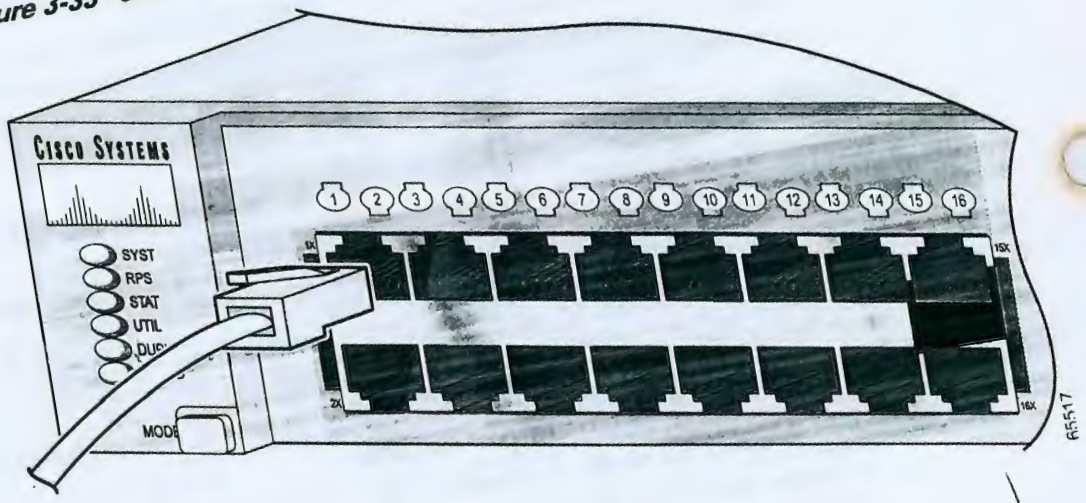


Figure 3-33 Connecting to a Port on Catalyst 2950G-48-EI Switches



CPMI - CORREI
088
Fls:
37
Doc:

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

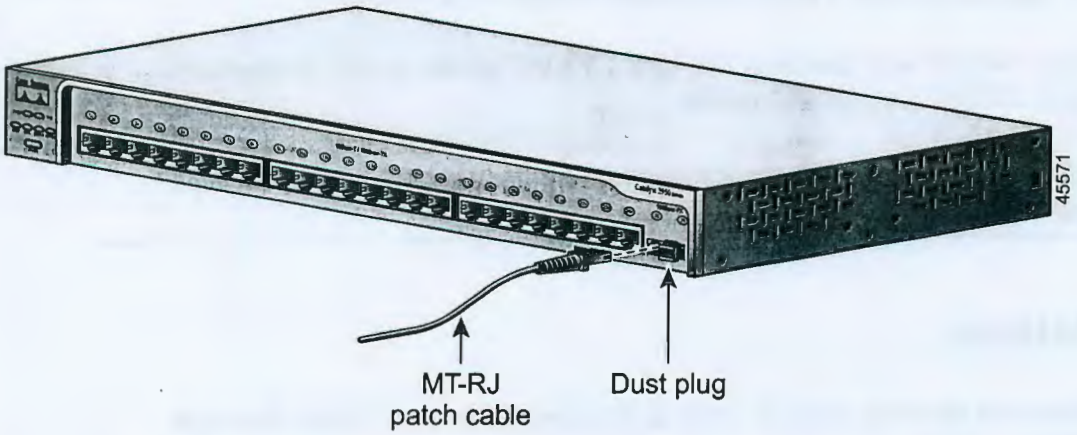
Caution Do not remove the dust plugs from the fiber-optic ports or the rubber caps from the fiber-optic cable until you are ready to connect the cable. The plugs and caps protect the fiber-optic ports and cables from contamination and ambient light.

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.

CPMI - CORREIOS
Fls: 0886
Doc: 3701

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*.

4.645
J

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.

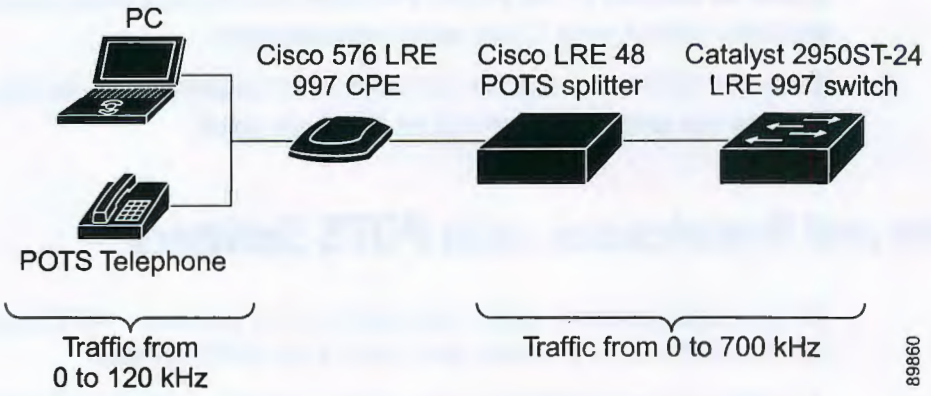
- We recommend that *you do not use* a Cisco LRE 48 POTS Splitter with a Catalyst 2950ST-24 LRE 997 switch and a Cisco 576 LRE 997 CPE as shown in Figure 3-35. Only traffic in a specific frequency range can be sent to and from the devices attached to the CPE.

  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.*

RQS 3-39 CPMI - CORREIOS
0887
Fls:
Doc: 3701

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



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.

U.643

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.

CPMI CORREIOS
3-41
0888
Fls:
Doc: 3701

Figure 3-36 Connecting to an LRE Port on a Catalyst 2950ST-8 LRE or 2950ST-24 LRE Switch

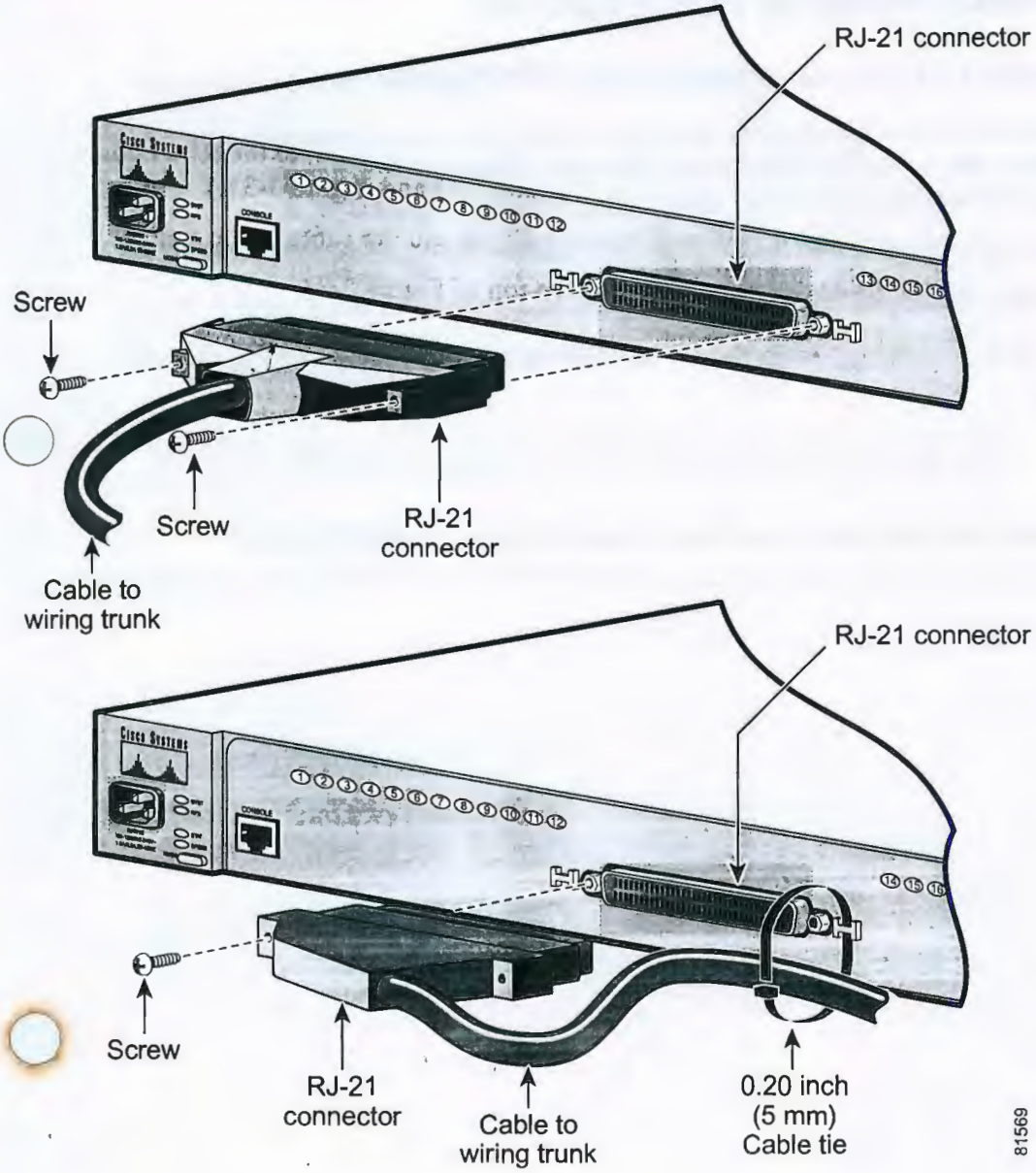
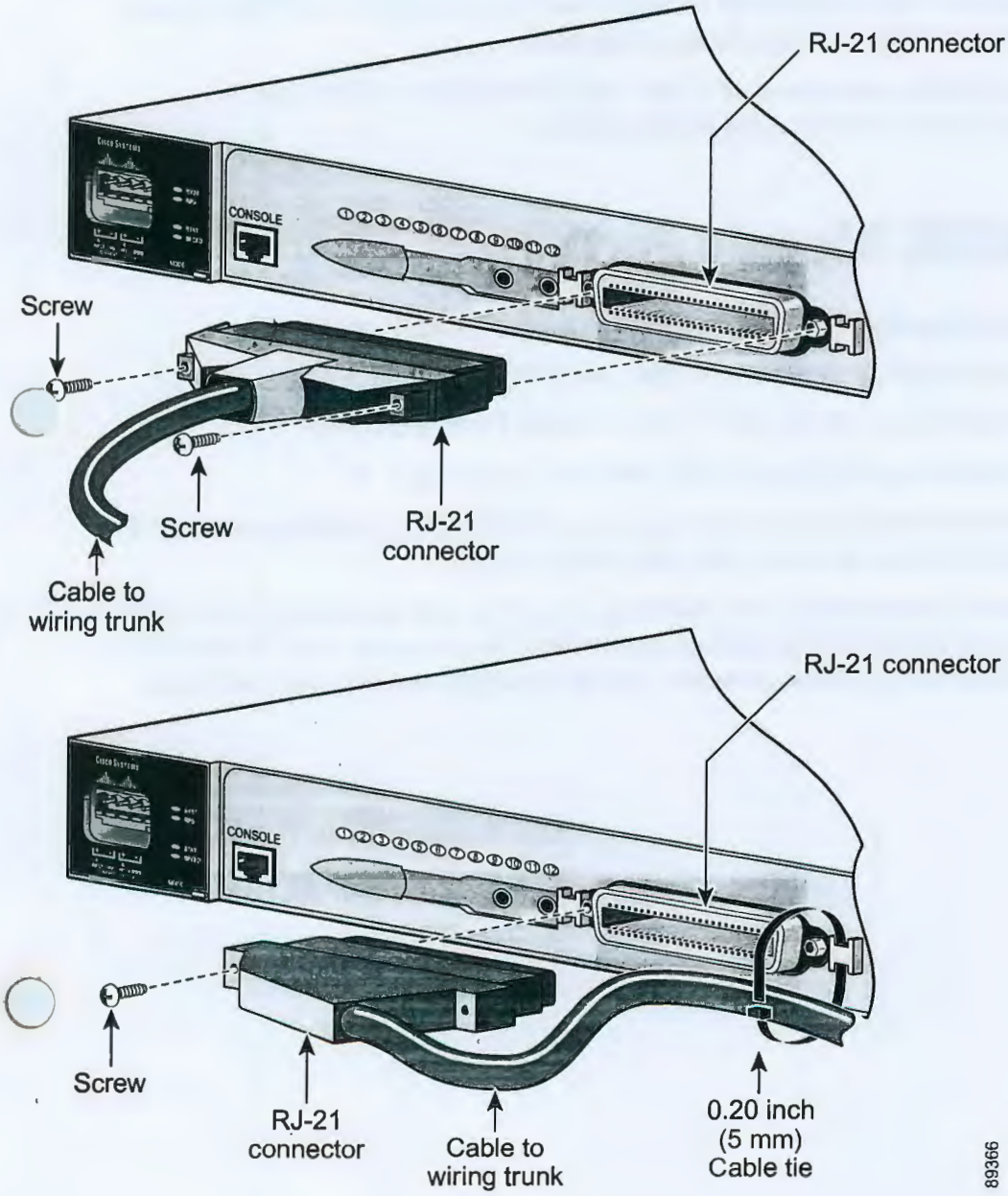


Figure 3-37 Connecting to an LRE Port on a Catalyst 2950ST-24 LRE 997 Switch



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.

ECT
4.639
J

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.

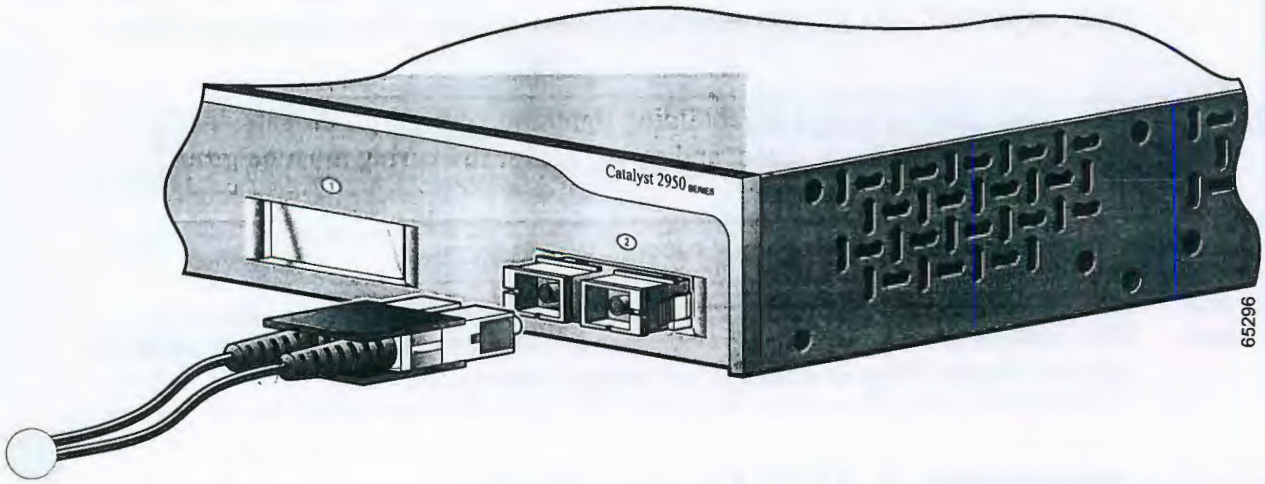
After installing the 1000BASE-X GBIC in the GBIC module slot, follow these steps:

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).

CPMI - CORREIOS
0890
Fls:
3701
Doc:

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.

E C T
1 4.637 1
CP 3
A

Connecting to 1000BASE-T GBIC Module Ports

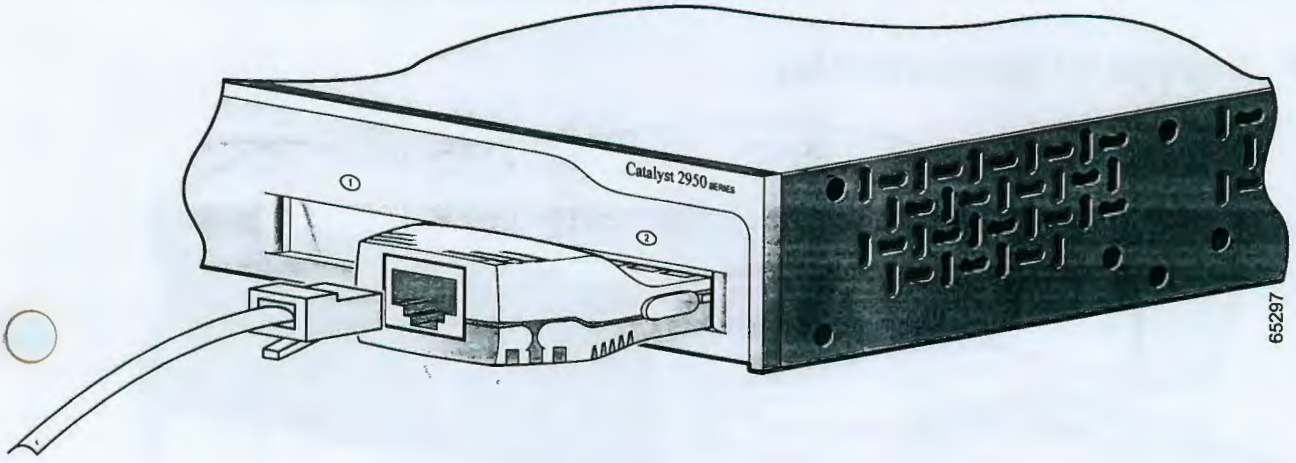
After installing the 1000BASE-T GBIC in the GBIC module slot, follow these steps:

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



CPMI 3-47
0891
Fls:
Doc: 3701

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.

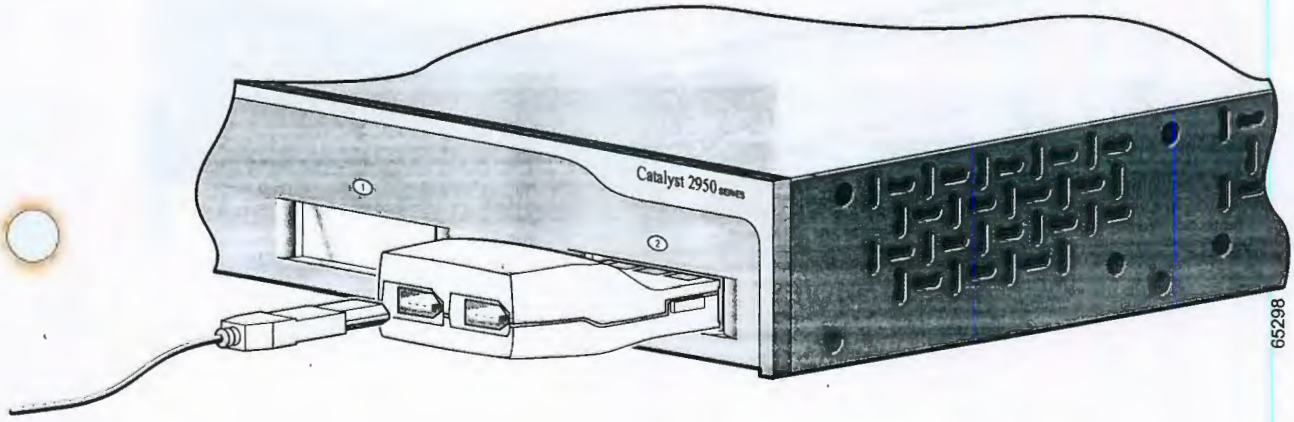
Step 4 Reconfigure and restart the switch or target device, if necessary.

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



4.635

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.

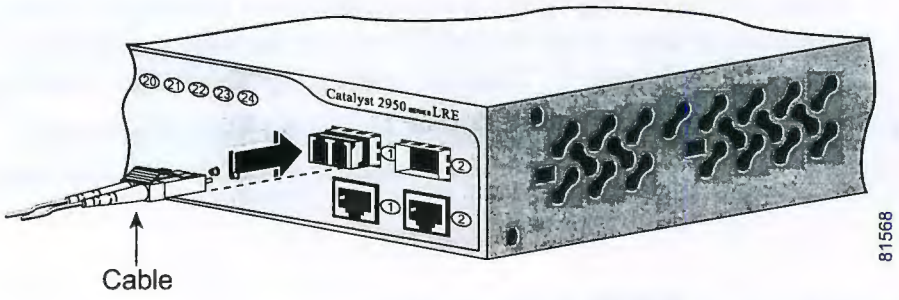
CPMI - CORREIOS
0892
Fls:
3701
Doc:

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 CA

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 0893
Doc: 3701

ECT
4.633
J

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

POS-MG/2005 - CN
CPMI - CORREIOS
Fls: 0894
Doc: 3701

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

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 Series Switch is combined with the Cisco Redundant Power System (RPS) 300 or RPS 675 for protection against internal 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, and 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.

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

4.631
J

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

CPMI - CORREIOS
Fls: 0895
Doc: 3701

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

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,

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

ECT 4.629 J

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.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0896
Fls:
Doc: 3701

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement

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.

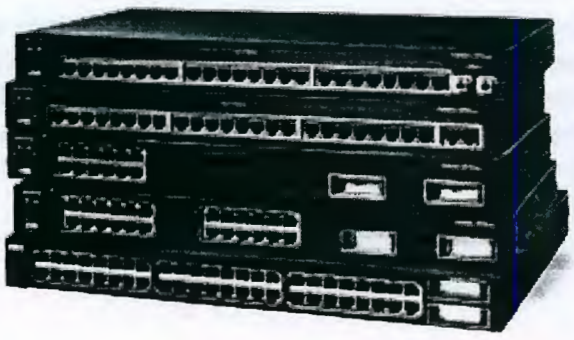
Cisco CMS Software supports standards-based connectivity options such as Ethernet, Fast Ethernet, Fast EtherChannel, Gigabit Ethernet, and Gigabit EtherChannel connectivity. Because Cisco switch clustering technology is not limited to a single stack of switches, Cisco CMS Software expands the traditional cluster domain beyond a 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



All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

4.627
J
CPMI - AC

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)

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 0897
Doc: 3701

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

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.

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

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.

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

4.625 J DSI - AC

REQS Nº 03/2003 - CN
CPMI - CORREIOS
Fls: 0898
Doc: 3701

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	

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

4.623
J
CPI - AC

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	

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 0899
Doc: 3701

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

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).

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

4.621
J

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

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

ROS Nº 03/2005 - CN
CPMI - CORREIOS
0900
Fls:
3701
Doc:

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

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

4.619

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.

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

CPMI - CORREIOS
0901
Fls:
3701
Doc:

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

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

ECT 4.617 J CPL-AS

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

CPMI - CORREIOS
0902
Fls:
Doc: 3701

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

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

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

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Aironet, Catalyst, Cisco, Cisco IOS, Cisco Systems, the Cisco Systems logo, EtherChannel, GigaStack, SMARTnet, and SwitchProbe are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0304R)

BU/LW4574 05/03

Apenace CD

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 0903
Doc: 3701

Cisco Systems

ECT 4.615 J CPI-AC

Data Sheet

Cisco Catalyst 2950 Series Switches with Cisco **Standard** Image Software

Product Overview

The Cisco® Catalyst® 2950SX-24, 2950-24, and 2950-12 switches are members of the Cisco Catalyst 2950 Series and are standalone, fixed-configuration, managed 10/100 switches that provide basic workgroup connectivity for small to medium-sized networks. These wire-speed desktop switches come with Cisco Standard Image (SI) Software features and offer Cisco IOS® functioning for basic data, video, and voice services at the edge of the network. Embedded in all 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.

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 SI Software offers Cisco IOS Software functioning for basic data, video, and voice services. For networks that require additional security, advanced quality of service (QoS), and high availability, Cisco Enhanced Image (EI) Software delivers intelligent services such as rate limiting and security filtering for deployment at the network edge. The Cisco Catalyst 2950SX-24, 2950-24, and 2950-12 switches are only available with Cisco SI Software for the Cisco Catalyst 2950 Series.

- Cisco Catalyst 2950SX-24 Switch—24 10/100 ports with 2 fixed 1000BASE-SX uplinks
- Cisco Catalyst 2950-24 Switch—24 10/100 ports
- Cisco Catalyst 2950-12 Switch—12 10/100 ports

These switches provide customers with a choice of connectivity options. While Cisco Catalyst 2950-12 and 2950-24 switches provide 12 and 24 10/100 ports for edge connectivity, respectively, Cisco Catalyst 2950SX-24 switches provide 24 10/100 ports and 2 integrated 1000BASE-SX ports for gigabit uplink connectivity over fiber. With these integrated ports, customers get an extremely cost-effective solution for delivering gigabit speeds using fiber. Dual ports also provide redundancy and increased availability—and a cost-effective means for cascading switches and managing them as a cluster. This switch is ideal for education and government segments, where fiber uplinks are a requirement.

Cisco Catalyst 2950 Series intelligent Ethernet switches with Cisco EI Software are also part of the Cisco Catalyst 2590 Series. These fixed-configuration, stackable models bring intelligent services, such as advanced QoS, enhanced security, and high availability, to the network edge—while maintaining the simplicity of traditional LAN switching. When a Cisco Catalyst

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0904
Fls:
Doc: 3701

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

2950 Series Intelligent Ethernet Switch is combined with a Cisco Catalyst 3550 Series Switch, the solution enables IP routing from the edge to the core of the network. Refer to the Cisco Catalyst 2950 Series Switches with Cisco Enhanced Image Software data sheet for more information.

Network Availability with Wire-Speed Performance in Connecting End Stations to the LAN

With a switching fabric of 8.8 Gbps and a maximum forwarding bandwidth of 4.4 Gbps, Cisco Catalyst 2950 Series switches deliver wire-speed performance on all ports in connecting end stations and users to the company LAN. With basic services, these switches support performance-boosting features such as Fast EtherChannel®— offering up high-performance bandwidth between Cisco Catalyst switches, routers, and servers.

Network Security

Cisco Catalyst 2950 Series switches offer enhanced data security through numerous security features. These features allow customers to provide network security based on users or Media Access Control (MAC) addresses. The security enhancements are available free of charge by downloading the latest software release for Cisco Catalyst 2950 Series switches.

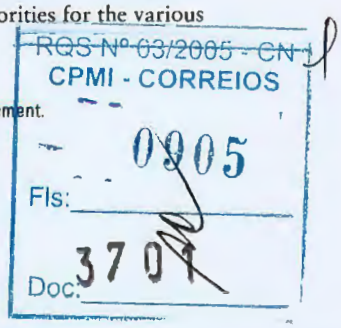
The Private VLAN Edge feature isolates ports on a switch, helping to ensure that traffic travels directly from the entry point to the aggregation device through a virtual path and that it cannot be directed to another port. In addition, for authentication of users with a Terminal Access Controller Access Control System (TACACS+) or a Remote Authentication Dial-In User Service (RADIUS) server, 802.1x provides port-level security. Simple Network Management Protocol Version 3 (SNMPv3) (non-crypto) monitors and controls network devices and manages configurations, performance, collection of statistics, and security.

With the Cisco Catalyst 2950SX-24, 2950-24, and 2950-12 switches, network managers can implement high levels of port and console security. MAC-address-based port-level security prevents unauthorized stations from accessing the switch. Multilevel access security on the switch console and the Web-based management interface prevent unauthorized users from accessing or altering switch configuration, and can be implemented using an internal user database on each switch, or a centrally administrated TACACS+ or RADIUS server. 802.1x, in conjunction with a RADIUS server, allows for dynamic port-based user authentication. In addition, 802.1x can coexist with port security on a per-port basis. 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 or portion of the network, or restrict the applications used in certain areas of the network.

Network Control

The Cisco Catalyst 2950SX-24, 2950-24, and 2950-12 switches deliver LAN-edge QoS, supporting two modes of reclassification. One mode—based on the IEEE 802.1p standard—honors the class-of-service (CoS) value at the ingress point and assigns the packet to the appropriate queue. In the second mode, packets can be reclassified based on a default CoS value assigned to the ingress port by the network administrator. In the case of frames that arrive without a CoS value (such as untagged frames), these switches support classification based on a default CoS value per port assigned by the network administrator. Once the frames have been classified or reclassified using one of the above modes, they are assigned to the appropriate queue at the egress port. These switches support four egress queues, which allow the network administrator to be more discriminating in assigning priorities for the various

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.



applications on the LAN. Strict Priority Scheduling configuration helps ensure that time-sensitive applications (such as voice) always follow an expedited path through the switch fabric. Weighted Round Robin (WRR) scheduling, another significant enhancement, ensures that lower-priority traffic receives attention without comprising the priority settings administered by a network manager. These features allow network administrators to prioritize mission-critical, time-sensitive traffic, such as voice (IP telephony traffic), enterprise resource planning (ERP) (Oracle, SAP, and so on), and CAD/CAM over less time-sensitive applications such as File Transfer Protocol (FTP) or e-mail (SMTP).

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, these 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) table entry.

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 virtual LAN (VLAN).

Per VLAN Spanning-Tree Plus (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.

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 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 a single wiring closet and saves time and effort for network administrators.

Cisco Systems, Inc.
All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0906
Fls: 3701
Doc:

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. 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. Figures 1–3 show Cisco Catalyst 2950 Series switches.

Figure 1
Cisco Catalyst 2950-12 Switch

Figure 2
Cisco Catalyst 2950-24 Switch

Figure 3
Cisco Catalyst 2950SX-24 Switch

Cisco Systems, Inc.
All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0907
Fls:
Doc: 370.1

Product Features and Benefits

Table 1 lists the features and benefits of 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. • 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. • 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 through Cisco 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. • 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, and fast-join and immediate leave are available as enhancements.

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS Nº 03/2005 - CPMI - CORREIOS
0908
Fls:
3701
Doc:

ECT
4.610
CPL - AC

Feature	Benefit
Security	
Network-wide security features	• A private VLAN edge provides security and isolation between ports on a switch, ensuring that voice traffic travels directly from its entry point to the aggregation device through a virtual path and 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. It provides unique benefits to customers who have a large base of mobile (wireless) users accessing the network, including: . 802.1x with Voice VLAN to give a Cisco IP Phone access to the voice VLAN regardless of the authorized or unauthorized state of the port. 802.1x with port security for authenticating the port and managing network access for all MAC addresses, including that of the client. • 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. • Multilevel security on console access prevents unauthorized users from altering the switch configuration. • Trusted Boundary provides the ability to trust the QoS priority settings if an IP phone is present and disable the trust setting in the event that the IP phone is removed, thereby preventing a rogue user from overriding prioritization policies in the network.
QoS	
Layer 2 QoS	• Support for reclassifying frames based either on 802.1p CoS value or default CoS value per port assigned by network manager. • 4 queues per egress port supported in hardware. • The WRR scheduling 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.

Cisco Systems, Inc.
All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0909
Fls:
Doc: 3701

Feature	Benefit
Management	
Superior manageability	• SNMP and Telnet interface support deliver comprehensive in-band management, and a command-line interface (CLI)-based management console provides detailed out-of-band management. • An embedded Remote Monitoring (RMON) software agent supports 4 RMON groups (history, statistics, alarms, and events) for enhanced traffic management, monitoring, and analysis. • A Switched Port Analyzer (SPAN) port can mirror traffic from 1 or many ports to another port for monitoring all 9 RMON groups with an RMON probe or network analyzer. • 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. • 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. • Crash Information support enables the switch to generate a crash file for improved troubleshooting. • Show Interface Capabilities provides information on the configuration capabilities of any interface. • The RTTMON Management Information Base (MIB) allows users to monitor network performance between a Cisco Catalyst switch and a remote device.
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 ensures that any combination of the above switches can be managed with a Cisco Catalyst 2950 Series switch. • Cisco AVVID (Architecture for Voice, Video and Integrated Data) 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). • 1-click software upgrades can be performed across the entire cluster simultaneously, and configuration cloning enables rapid deployment of networks. • 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 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.

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

4.609
RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 0910
3701
Doc:

Feature	Benefit
Support for CiscoWorks	• Manageable through CiscoWorks network management software on a per-port and per-switch basis providing 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.
Ease of use and ease of deployment	• Autoconfiguration eases deployment of switches in the network by automatically configuring multiple switches across a network via a bootp server. • Autosensing on each port detects the speed of the attached device and automatically configures the port for 10- or 100- operation, easing the deployment of the switch in mixed 10BASET and 100BASET environments. • Autonegotiating on all ports automatically selects half- or full-duplex transmission mode to optimize bandwidth. • 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. • Cisco Discovery Protocol versions 1 and 2 enable a CiscoWorks network management station to automatically discover the switch in a network topology. • Cisco VTP supports dynamic VLANs and dynamic trunk configuration across all switches. • Support for dynamic VLAN assignment through the implementation of the VLAN Membership Policy Server (VMPS) client function provides flexibility in assigning ports to VLANs. • Voice VLAN simplifies telephony installations by keeping voice traffic on a separate VLAN for easier network administration and troubleshooting. • The default configuration stored in Flash memory helps ensure that the switch can be quickly connected to the network and can pass traffic with minimal user intervention.

Product Specifications

Feature	Description
Performance	• 8.8-Gbps switching fabric • Cisco Catalyst 2950-12: 2.4 Gbps maximum forwarding bandwidth • Cisco Catalyst 2950-24: 4.8 Gbps maximum forwarding bandwidth • Cisco Catalyst 2950SX-24: 8.8 Gbps maximum forwarding bandwidth (Forwarding rates based on 64-byte packets) • Cisco Catalyst 2950-12: 1.8-Mpps wire-speed forwarding rate • Cisco Catalyst 2950-24: 3.6-Mpps wire-speed forwarding rate • Cisco Catalyst 2950SX-24: 6.6-Mpps wire-speed forwarding rate • 8-MB packet buffer memory architecture shared by all ports • 16 MB DRAM and 8 MB Flash memory • Configurable up to 8000 MAC addresses

Cisco Systems, Inc.
All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0911
Fls:
Doc: 3701

Feature	Description
Management	• BRIDGE-MIB • CISCO-2900-MIB • CISCO-BULK-FILE-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 • 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

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

4.607
RQS Nº 03/2005 - CN - CPMI - CORREIOS
0912
Fls:
3701
Doc:

Feature	Description
Standards	• IEEE 802.1x support • IEEE 802.3x full duplex on 10BASE-T and 100BASE-TX 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 802.3ad • IEEE 802.3z 1000BASE-X specification
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-SX ports: MT-RJ connectors, up to 550 meters of cable distance for 50/125 micron, or up to 275 meters of cable distance for 62.5/125 micron multimode fiber-optic cabling • Management console port: 8-pin RJ-45 connector, RJ-45-to-DB9 adapter cable 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 2950SX-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

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0913
Fls:
Doc: 3701

Feature	Description
Power connectors	Customers can provide power to a switch by using either the internal power supply or the Cisco Redundant Power System (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 connects 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 redundant power supply 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. • Only the Cisco RPS 300 (model PWR300-AC-RPS-N1) should be attached to the redundant power supply receptacle.
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 44.45 x 24.18 cm) • One rack-unit (RU) high (1.72 in./4.36 cm) • 6.5 lb (3.0 kg)
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)
Power requirements	• Power consumption: 30W (maximum), 102 BTUs per hour • AC input voltage/frequency: 100 to 127 or 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)	• 268,292 hours (Cisco Catalyst 2950-24) • 318,440 hours (Cisco Catalyst 2950-12) • 403,214 hours (Cisco Catalyst 2950SX-24)

Cisco Systems, Inc.
All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0914
Fls:
Doc: 3701

Feature	Description
Regulatory Agency Approvals	
Safety certifications	• UL 60950/CSA 22.2 No. 950 • IEC 60950/EN 60950 • AS/NZS 3260, TS001 • CE Marking
Electromagnetic emissions certifications	• FCC Part 15 Class A • EN 55022: 1998 (CISPR 22) Class A • EN 55022: 1998 (CISPR 22) • VCCI Class A • AS/NZS 3548 Class A • CE Marking • CNS 13438 Class A • CLEI Code • MIC
Warranty	• Lifetime limited 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

Cisco Systems, Inc.
All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0915
Fls:
Doc: 3701

Ordering Information

Model Numbers	Configuration
WS-C2950-12	• 12 10/100 ports • 1 RU standalone, fixed-configuration, managed 10/100 switch • Cisco SI Software
WS-C2950-24	• 24 10/100 ports • 1 RU standalone, fixed-configuration, managed 10/100 switch • Cisco SI Software
WS-C2950SX-24	• 24 10/100 ports with 2 fixed 1000BASE-SX uplinks • 1 RU standalone, fixed-configuration, managed 10/100 switch • Cisco SI Software

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

4.603
1

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

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Aironet, Catalyst, Cisco, Cisco IOS, Cisco Systems, the Cisco Systems logo, EtherChannel, and SMARTnet are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0304R)

BU/LW4574 05/03

PROC. Nº 08012.005 - CN
CPMI - CORREIOS
Fls: 0916
Doc: 3701

Apêndice CC

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 0917
Doc: 3791

Software Advisor

Major Release 12.2T

Product Family 3745

Releases 12.2(15)T

Feature Set IP PLUS IPSEC 3DES

ne features are dependent on product model, interface modules (i.e. Line ards & Port Adapters), and/or require a software feature license.

Your selections are supported by the following

Image Name	DRAM	Flash	Product Number	Options
c3745-ik9s-mz.12.2-15.T	128	32	S374CK9-12215T= S374CK9-12215T	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
ACL Sequence Numbering
ptive Frame Relay Traffic Shaping for Interface Congestion
Additional Vendor-Proprietary RADIUS Attributes
Address Resolution Protocol (ARP)
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 Multilink PPP Support on Multiple VCs
ATM Subinterface MIB/Traps
ATM SVC Troubleshooting Enhancements
ATM-DXI
AutoInstall Using DHCP for LAN Interfaces
Automatic modem configuration
AutoQoS - VoIP
Bandwidth Allocation Control Protocol (BACP)

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0918
Fls: 3701

Doc: 3701

ECT 4.601 J CPI-AG

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 Nonstop Forwarding (NSF) Awareness Support
BGP Policy Accounting
BGP Prefix-Based Outbound Route Filtering
BGP Route-Map Policy List Support
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
Call Release Source Reporting in Gateway-Generated Accounting Records
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
Certificate Security Attribute-Based Access Control
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
Cisco IOS Telephony Service (ITS) Version 2.01
Cisco IOS Telephony Service (ITS) Version 2.02
Cisco IOS Telephony Service (ITS) Version 2.1
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
Class-Based RTP & TCP Header Compression
Classless InterDomain Routing (CIDR) IP Default Gateway
Clear Channel T3/E3 with Integrated CSU/DSU
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
Conferencing and Transcoding for Voice Gateway Routers
Configurable per ATM-VC Hold Queue size
Configurable Timers in H.225
Connect-Info RADIUS Attribute 77
Content Engine Network Module for Caching and Content Delivery
Control Plane DSCP Support for RSVP
COPS for RSVP
Crashinfo Support
CT1/RBS (Robbed Bit Signaling)

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0919
Fls:
Doc: 3701

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 ODAP Server Support
DHCP On Demand Address Pool (ODAP) Manager for non-MPLS VPN pools
DHCP Option 82 Support for Routed Bridge Encapsulation
DHCP Proxy Client
DHCP Relay - MPLS VPN Support
DHCP Relay Agent Support for Unnumbered Interfaces
DHCP Secured IP Address Assignment
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
er profiles
er 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
DLR Enhancements: PGM RFC-3208 Compliance
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
w+ SNA Type of Service
Sw+ 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
Dynamic Multipoint VPN (DMVPN)
E1 R2 Signaling
Easy IP (Phase 1)
Easy VPN Remote Enhancements
Easy VPN Server
EIGRP Nonstop Forwarding (NSF) Awareness
Encrypted Vendor Specific Attributes
Enhanced Call and IVR Control for Rotary Call Set Ups
Enhanced Codec support for SIP using Dynamic Payloads
Enhanced IGRP (EIGRP)
Enhanced IGRP Stub Routing
Enhanced ITU-T G.168 Echo Cancellation
Enhanced Local Management Interface (ELMI)

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0920
Fls:
Doc: 3701

Enhanced Password Security
Enhanced Test Command
Enhanced Tracking Support.
Exporting and Importing RSA Keys
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
Flow-Based WRED
Frame Relay
Frame Relay - Multilink (MLFR-FRF.16)
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)
F e Relay Fragmentation with Hardware Compression
F e Relay FRF.9 Payload Compression
Frame Relay IP RTP Priority
Frame Relay Point-Multipoint Wireless
Frame Relay PVC Interface Priority Queueing
Frame Relay Queuing and Fragmentation at the Interface
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
Frame Relay Voice Adaptive Traffic Shaping
FUNI Support for Routers
FXO Answer and Disconnect Supervision
Gatekeeper Ecosystem Interoperability
Gateway Enhancements to Enable v4-v2 Interworking
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 Dual Tone Multifrequency (DTMF) Relay Using Named Telephone Events
H 3 Redundant Zone Support
H.323 Scalability and Interoperability Enhancements for Gateways
H.323 Support for Virtual Interfaces
H.323V4 Gateway Zone Prefix Registration Enhancements
H450.2 & H450.3 Support In IOS
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
HTTP 1.1 Web Server
HTTPS - HTTP with SSL 3.0
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

4.598
CPI-FC

IGMP State Limit
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)
'amed Access Control List
recedence 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 NAT Transparency
IPSec Network Security
IPSec Through Network Address Translation Support
IPSec Triple DES Encryption (3DES)
IPSec VPN Accounting
IPSec VPN High Availability Enhancements
IPv6 ADSL and Dial Deployment Support
IPv6 Extended Access Control List
IPv6 for Cisco IOS Software
IPv6 ISATAP Tunnel Support
IPv6 Quality of Service
ISDN
ISDN Advice of Charge (AOC)
ISDN Caller ID Callback
N Cause Code Override
ISDN Generic Transparency Descriptor (GTD) for Setup Message
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 Extended Failover
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)

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0922
Fls:
3301
Doc:

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
Low Latency Queuing (LLQ) for IPSEC Encryption Engines
LSDO: L2TP Large-Scale Dial-Out
MAC Address Filtering
Malicious Caller Identification (MCID) Invocation Support for Enterprise Ne...
Manual certificate enrollment (TFTP and cut-and-paste)
MD5 File Validation
Measurement-Based Call Admission Control for SIP
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 - Challenge/Response Extestions
Mobile IP - Dynamic DNS and Multiple DHCP Support
Mobile IP - Fastswitching Support on FA
Mobile IP - Generic NAI Support and Home Address Allocation
Mobile IP - HA Accounting
Mobile IP - HA Policy Routing
Mobile IP - HMAC-MD5 support
Mobile IP - IPSec for HA-FA Tunnel
Mobile IP - Mobile Networks
Mobile IP - Mobile Networks Asymmetric Link and Dynamic Network
Mobile IP - Mobile Networks Priority HA Assignment
Mobile IP - Mobile Networks Static Collocated Care of Address
Mobile IP - Mobile Networks Tunnel Templates for Multicast
Mobile IP - NAT Detect
Mobile IP - Private Addressing Support
Mobile IP - Proxy Mobile IP and Proxy CHAP
Mobile IP - Single IDB Tunnel Support
Mobile IP - Support for FA Reverse Tunnelling
Mobile IP - Support NAI Based MNs that are serviced by many HAs
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)
Modular QoS CLI (MQC) - Based Frame Relay Traffic Shaping
Modular QoS CLI (MQC) Three-Level Hierarchical Policer
Modular QoS CLI (MQC) Unconditional Packet Discard
MPLS VPN support for EIGRP between Provider Edge (PE) and Customer Edge (CE...
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)
Multicast Subsecond Convergence
Multichassis MultiLink PPP (MMP)
Multiclass Multilink PPP
Multihop VPDN
Multilink PPP
Multilink PPP Enable/Disable via Radius for Preauthentication User
Multiple RSA Keypair Support

ECT 4.596 1

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 Default Inside Server Enhancement
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)
Flow 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 for IPv6
OSPF Forwarding Address Suppression in Translated Type-5 LSAs
OSPF Inbound Filtering using Route Maps with a Distribute List
OSPF Nonstop Forwarding Awareness
OSPF Not-So-Stubby Areas (NSSA)
OSPF On Demand Circuit (RFC 1793)
OSPF Packet Pacing
OSPF Sham-Link Support for MPLS VPN
OSPF Shortest Paths First Throttling
OSPF Stub Router Advertisement
OSPF Support for Fast Hellos
OSPF Support for Multi-VRF on CE Routers
OSPF Update Packet-Pacing Configurable Timers
Packet Classification Based on Layer3 Packet-Length
Packet Classification using Frame-Relay DLCI Number
PAD Subaddressing
Parse Bookmarks
Parser Cache
Password Authentication Protocol (PAP)
Per-User Configuration
Percentage-Based Policing and Shaping
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)
PPP
PPP over ATM
PPP over ATM (IETF-Compliant)
PPP over ATM SVCs
PPP Over Fast Ethernet 802.1Q
PPP over Frame Relay

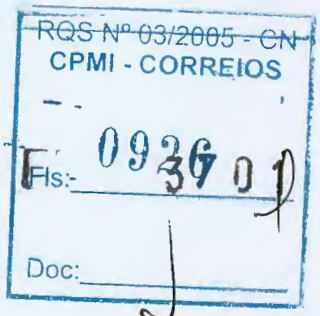
RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 0924
Doc: 3791

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)
Privilege Command Enhancement
Protocol Translation (PT)
PSTN Fallback
QoS Device Manager (QDM)
QoS for Virtual Private Networks
QoS Packet Marking
QoS Priority Percentage CLI Support
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 Centralized Filter Management
RADIUS for Multiple User Datagram Protocol Ports
RADIUS Interim Update at Call Connect
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 Path Forwarding - Source Exists only
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
Routing Through Dial Strings
RSVP - ATM Quality of Service (QoS) Interworking
RSVP - Resource Reservation Protocol
RSVP Local Policy Support
RSVP Message Authentication
RSVP Refresh Reduction and Reliable Messaging
RSVP Scalability Enhancements
RSVP Support for Frame Relay
RSVP support for LLQ
RSVP Support for RTP Header Compression
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
Selective Packet Discard (SPD)
Selective Virtual-Access Interface Creation
Service Assurance Agent (SAA) APM Application Performance Monitor
Service Assurance Agent (SAA) DHCP Operation
Service Assurance Agent (SAA) Distribution of Data

ECT 4.595 J

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0925
Fls:
3701
Doc:

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
Settlement for Packet Telephony
Settlement for Packet Telephony - Roaming & PKI Multiple Roots
Shell-Based Authentication of VPDN Users
Show Command Redirect
Single Rate 3-Color Marker for Traffic Policing
SIP - Call Transfer Enhancements Using Refer Method
- Call Transfer Using Refer Method
- 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 and H.323 Fax Enhancements
SIP Carrier Identification Code
SIP Diversion Header Implementation for Redirecting Number
SIP Enhanced 180 Provisional Response Handling
SIP Extensions for Caller Identity and Privacy
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 Redirect Processing Enhancement
SIP Session Timer Support
SIP Support for Media Forking
SIP T.37 and Cisco Fax
SIP T.38 Fax Relay
SIP: Core SIP Technology Enhancements
ISDN Suspend/Resume Support
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
Software IPPCP (LZS) with Hardware Encryption
Source Interface Selection for Outgoing Traffic with Certificate Authority ...
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
SRST: Survivable Remote Site Telephony Version 2.02



SRST: Survivable Remote Site Telephony Version 2.1
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
T[illegible] Ring ISL
T[illegible]n 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
UDP forwarding support of IP Redundancy Virtual Router Group (VRG)
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[illegible] Support
V.92 Modem on Hold
V.92/V.44 Support for Digital Modems
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 Call Tuning
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

ECT 4.59 J

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 0927
3701
Doc:

4.592
J

VoIP Outgoing Trunk Group Identification and Carrier ID for Gateways
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 Dual Serial Line Management
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
5 Switch Local Acknowledgement
5 Switching between PVCs and SVCs
X.25 Terminal Line Security for PAD Connections
X.28 Emulation
XGCP Bind Command for Control and Media Packets

To find out more about your selected release, you can use the Bug Toolkit

Close Window

© 1992-2003 Cisco Systems, Inc. All rights reserved. Important Notices, Privacy Statement, and Trademarks of Cisco Systems, Inc.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0928
Fls:
3704
Doc:

Apêndice CD

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0929
Fls: 3701
Doc:

4-591
CPI-AC

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

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls 3730
Doc:

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

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, and 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

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

4.589
J

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

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0931
Fls:
3701
Doc:

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

- 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 engines
- 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

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

4.587
1

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

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0932
Fls:
3701
Doc:

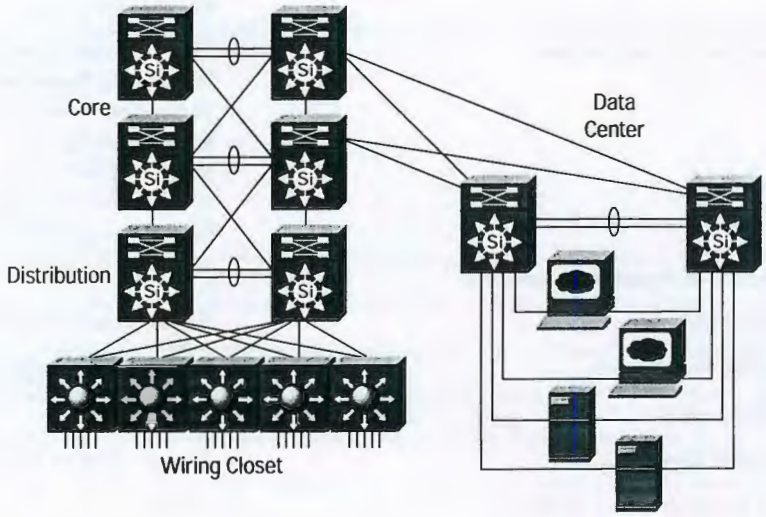
All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

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

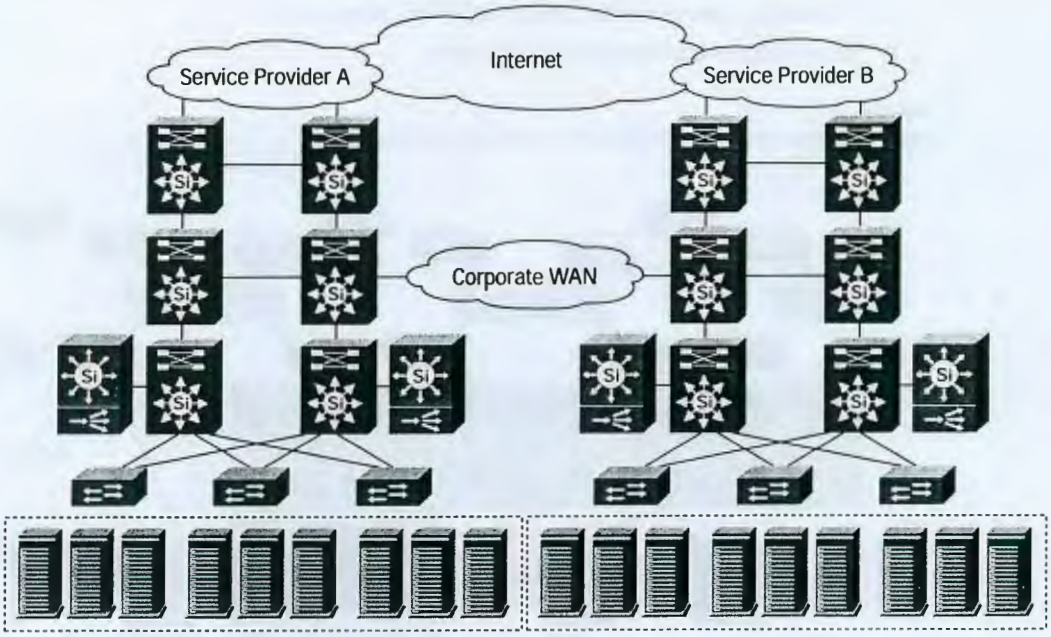


All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

21.585
J

- [*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

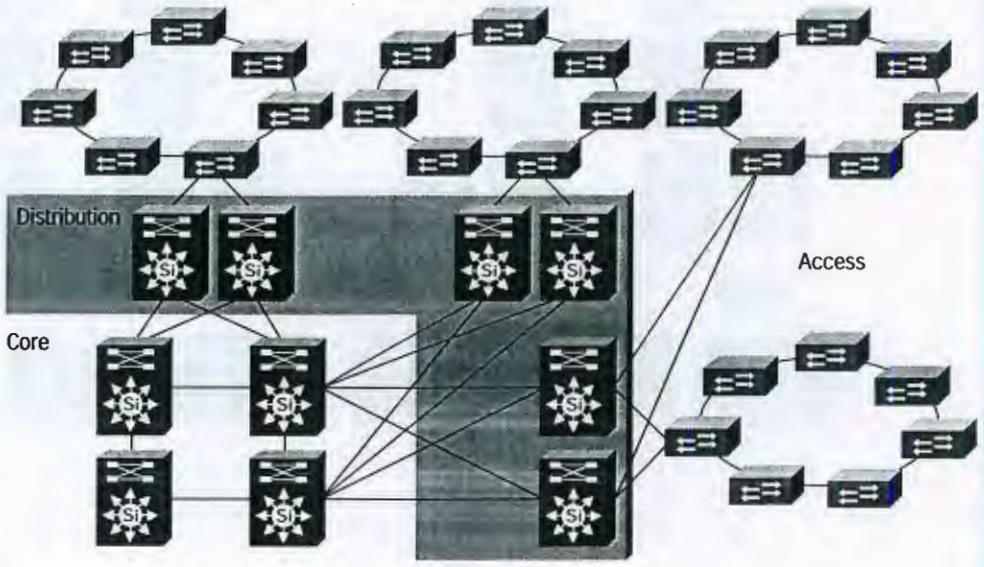


RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls: 0933
Doc: 3701

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

- *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

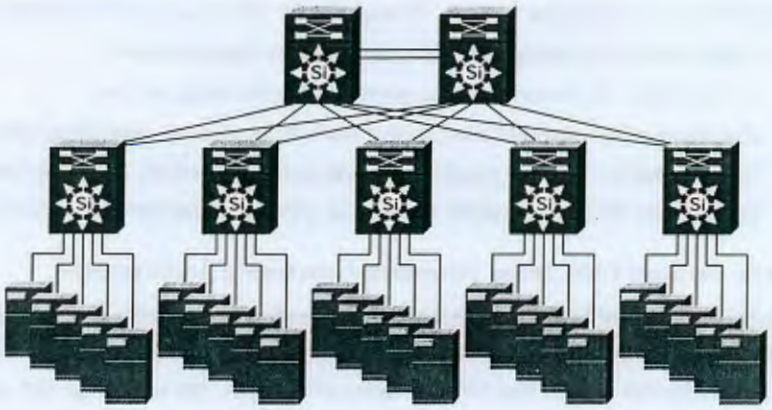


Cisco Systems, Inc.
All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

4.583

- *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



Cisco Systems, Inc.
All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

ROS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 0934
Doc: 3701

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 Systems, Inc.
All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

4.581
J

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.

DOC/INFO 2005 - CN
CPMI - CORREIOS
0935
Fls:
3201
Doc:

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

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 720
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

Cisco Systems, Inc.
All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

4.579

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

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 0936
Doc: 3701

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

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

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

- *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.

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0937
Fls:
3701
Doc:

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

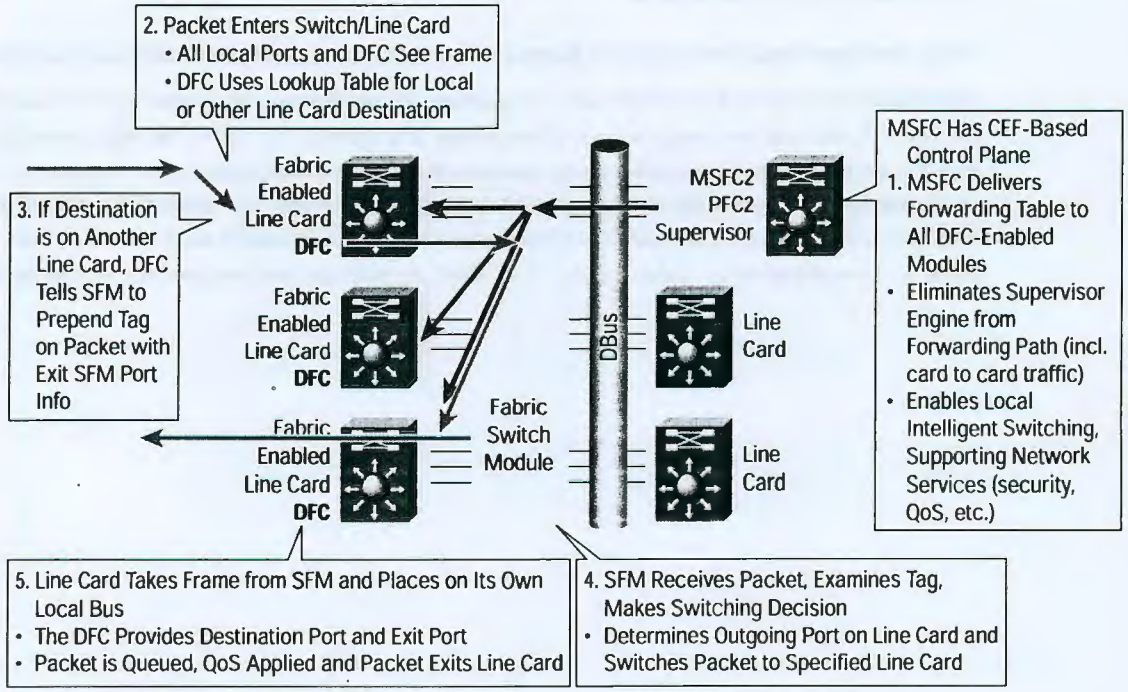
With Distributed Cisco Express Forwarding (dCEF), forwarding engines located on the interface modules make forwarding decisions locally and in parallel, allowing the Cisco Catalyst 6500 Series to achieve the highest forwarding rates in the industry. With dCEF, forwarding occurs on the interface modules in parallel and system performance scales up to 400 Mpps—the aggregate of all forwarding engines working together.

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

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



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 Systems, Inc.
All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0938
Fls: 3701
Doc:

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.

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

H.573
1

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.

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS Nº 03/2005 - CN
GEMI - CORREIOS
0939
Fls:
3701
Doc:

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 edge
- *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.

Cisco Systems, Inc.
All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

4.571

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

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0940
Fls:
3701
Doc:

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

Cisco Systems, Inc.
All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

4.569
1

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

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0941
Fls: 3701
Doc:

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

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

4567
3

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

ROS Nº 03/2005 - CN
CPMI - CORREIOS
0942
Fls:
3701
Doc:

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

OTT 4.566 J

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	Host extensions, Distance Vector Multicast Routing Protocol (DVMRP)
	2236	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

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

4.565

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

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0943
Fls: 3701
Doc:

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

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

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

21.563
J

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

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0944
Fls: 3701
Doc:

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)

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

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

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0945
Fls:
Doc: 3701

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

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Catalyst, Cisco, Cisco Systems, Cisco IOS, the Cisco Systems logo, EtherChannel, and SMARTnet are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0304R)

MH/LW4273 0403

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 0946
Doc: 3761

4.559

VPN Client User Guide for Windows

Release 3.6
August 2002

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

Text Part Number: 78-14738-01
Customer Order Number: DOC-7814738=

RQS Nº 03/2005 - CPMI - CORREIOS
0947
Fls:
3701
Doc:

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED 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.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

CCIP, the Cisco Arrow logo, the Cisco *Powered* Network mark, the Cisco Systems Verified logo, Cisco Unity, Follow Me Browsing, FormShare, Internet Quotient, iQ Breakthrough, iQ Expertise, iQ FastTrack, the iQ Logo, iQ Net Readiness Scorecard, Networking Academy, ScriptShare, SMARTnet, TransPath, and Voice LAN are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, Discover All That's Possible, The Fastest Way to Increase Your Internet Quotient, and iQuick Study are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherSwitch, Fast Step, GigaStack, IOS, IP/TV, LightStream, MGX, MICA, the Networkers logo, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, RateMUX, Registrar, SlideCast, StrataView Plus, Stratm, SwitchProbe, TeleRouter, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0206R)

VPN Client User Guide for Windows
Copyright © 2002, Cisco Systems, Inc.
All rights reserved.

4.557
J

CONTENTS

Preface ix

Audience ix

Organization ix

Terminology x

Related documentation x

VPN 3000 Series Concentrator Documentation xi

Conventions xi

Data Formats xii

Obtaining Documentation xiii

World Wide Web xiii

Documentation CD-ROM xiii

Ordering Documentation xiii

Documentation Feedback xiii

Obtaining Technical Assistance xiv

Cisco.com xiv

Technical Assistance Center xiv

Cisco TAC Web Site xv

Cisco TAC Escalation Center xv

CHAPTER 1 **Understanding the Cisco VPN Client** 1-1

How the VPN Client Works 1-2

Connection Technologies 1-2

VPN Client Features 1-3

Program Features 1-3

Windows NT, Windows 2000, and Windows XP Features 1-3

IPSec Features 1-4

Authentication Features 1-4

Firewall Features 1-5

VPN Client IPSec Attributes 1-5

CHAPTER 2 **Installing the VPN Client** 2-1

Installation Applications 2-1

Verifying System Requirements 2-1

Gathering Information You Need 2-2

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls: 0548
Doc: 3701

Installing the VPN Client Through InstallShield 2-3
Installing the VPN Client Through Microsoft Windows Installer 2-5
What Next? 2-9

CHAPTER 3 **Configuring the VPN Client** 3-1
How to Get Help 3-1
Determining the VPN Client Version 3-3
What Is a Connection Entry? 3-5
How To Create a New Connection Entry 3-5
Choosing an Authentication Method 3-7
Group Authentication 3-7
Certificate Authentication 3-8
Sending a Certificate Authority Certificate Chain 3-9
Validating a Certificate 3-10
Configuring an Entrust Certificate for Authentication 3-10
Configuring a Connection Entry for a Smart Card 3-11
Smart Cards Supported 3-12
Completing the Connection Wizard 3-13
What Next? 3-13
Setting or Changing Connection Entry Properties 3-14
Changing General Settings 3-17
Changing Connection Entry Description 3-17
Enabling Transparent Tunneling 3-17
Allowing Local LAN Access 3-18
Adjusting the Peer Response Timeout Value 3-19
Logging on to Microsoft Network (Windows 95, Windows 98, and Windows ME) 3-20
Changing Authentication Settings 3-20
Changing Group Name or Group Password 3-21
Choosing a Different Certificate 3-22
Changing Connection Settings 3-23
Enabling and Adding Backup Servers 3-23
Removing Backup Servers 3-24
Changing the Order of the Servers 3-24
Disabling Backup Servers 3-24
Configuring a Connection to the Internet Through Dial-up Networking 3-24
Microsoft Dial-up Networking 3-25
Third Party Dial-up Program 3-26
Changing the VPN Device Address for a Connection Entry 3-26

4.555
J

CHAPTER 4 **Connecting to a Private Network** 4-1

Starting the VPN Dialer 4-2

Connection Procedure 4-2

Using the VPN Client to Connect to the Internet via Dial-Up Networking 4-3

Authenticating to Connect to the Private Network 4-4

User Authentication 4-5

Authenticating Through the VPN Device Internal Server or RADIUS Server 4-5

Authenticating Through a Windows NT Domain 4-6

Changing your Password 4-7

Authenticating Through RSA Data Security (RSA) SecurID (SDI) 4-8

RSA User Authentication: SecurID Tokencards (Tokencards, Pinpads, and Keyfobs) and SoftID v1.0 (Windows 95, Windows 98, and Windows ME) 4-8

RSA User Authentication: SoftID v1.x (Windows NT Only) and SoftID v2.0 (All Operating Systems) 4-9

RSA New PIN Mode 4-9

SecurID Next Cardcode Mode 4-11

Connecting with Digital Certificates 4-11

Connecting with an Entrust Certificate 4-12

Accessing Your Profile 4-12

Entrust Inactivity Timeout 4-14

Using Entrust SignOn and Start Before Logon Together 4-14

Connecting with a Smart Card or Token 4-14

Completing the Private Network Connection 4-16

Using Automatic VPN Initiation 4-16

Connecting Through Auto Initiation 4-17

Disconnecting Your Session 4-19

Changing Option Values While Auto Initiation is Suspended 4-20

Disabling Auto Initiation 4-20

Disabling While Suspended 4-21

Restarting After Disabling Auto Initiation 4-21

Connection Failures 4-22

Summary of Auto Initiation States 4-23

Viewing Connection Status 4-24

General Information 4-24

Statistics 4-26

Secured Routes 4-27

Local LAN Routes 4-27

Time Connected 4-27

Firewall Tab 4-27

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0919
Fls:
Doc: 3701

AYT Firewall Tab 4-28
Centralized Protection Policy (CPP) Using the Cisco Integrated Client 4-29
Firewall Rules 4-29
Client/Server Firewall Tab 4-31
Resetting Statistics 4-32
Closing the VPN Client 4-32
Disconnecting your VPN Client Connection 4-32

CHAPTER 5 **Managing the VPN Client** 5-1
Managing VPN Client Connection Entries 5-2
Cloning a Connection Entry 5-3
Deleting a Connection Entry 5-4
Renaming a Connection Entry 5-5
Importing a VPN Client Configuration File 5-5
Erasing a Saved Password for a Connection Entry 5-7
Creating a Shortcut for a Connection Entry 5-10
Enabling Stateful Firewall (Always On) 5-11
Launching an Application 5-11
Managing Windows NT Logon Properties 5-14
Starting a Connection Before Logging on to a Windows NT Platform 5-14
What Happens When You Use Start Before Logon 5-15
Turning Off Start Before Logon 5-15
Permission to Launch an Application Before Log On 5-15
Disconnecting When Logging Off of a Windows NT Platform 5-16
Managing Auto Initiation 5-16
Viewing and Managing the VPN Client Event Log 5-17
Starting the Log Viewer 5-18
Displaying the Version of the Software 5-19
Collecting Events 5-19
Filtering Events 5-20
Searching the Log File 5-22
Printing the Log File 5-23
Saving the Log File 5-24
Clearing the Events Display 5-24
Receiving Notifications From a VPN Device 5-25
Upgrade Notifications 5-25
Firewall Notifications 5-26
Upgrading the VPN Client Software (InstallShield) 5-27

4.553

Upgrading the VPN Client Software (MSI) 5-29
Uninstalling the VPN Client with the Uninstall Application 5-29
Removing the VPN Client Software MSI Installation 5-32

CHAPTER 6 **Enrolling and Managing Certificates** 6-1
Starting Certificate Manager 6-2
What are Certificate Stores? 6-3
Enrolling for a Certificate 6-4
Enrollment Form 6-4
Starting Enrollment 6-5
Enrolling Through the Network 6-6
Enrolling Through a File Request 6-11
Importing a Certificate File 6-15
Managing Personal and CA/RA Certificates 6-17
Viewing a Certificate 6-18
Verifying a Certificate 6-20
Deleting a Certificate 6-21
Changing the Password on a Personal Certificate 6-22
Exporting a Certificate 6-23
Managing Enrollment Requests 6-25
Viewing the Enrollment Request 6-26
Deleting an Enrollment Request 6-27
Changing the Password on an Enrollment Request 6-28
Completing an Enrollment Request 6-29

APPENDIX A **Copyrights and Licenses** A-1
Client Software License Agreement of Cisco Systems A-1
RSA software A-2
Zone Labs A-3

INDEX

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0250
Fls:
3701
Doc:

4.551

Preface

This *VPN Client User Guide* tells you how to install, use, and manage the Cisco VPN Client with Cisco Systems products.

Audience

This guide is for users of remote clients who want to set up virtual private network (VPN) connections to a central site. Network administrators can also use this guide for information about configuring and managing VPN connections for remote clients. We assume that you are familiar with the Windows platform and know how to use Windows applications. A network administrator should be familiar with Windows system configuration and management and know how to install, configure, and manage internetworking systems. For information specific to a network administrator, see *VPN Client Administrator Guide*.

Organization

This guide is organized as follows:

Chapter	Title	Description
Chapter 1	Understanding the Cisco VPN Client	Explains briefly what the VPN Client is and how it works.
Chapter 2	Installing the VPN Client	Tells you how to install the VPN Client.
Chapter 3	Configuring the VPN Client	Tells you how to configure the VPN Client, including setting optional parameters.
Chapter 4	Connecting to a Private Network	Tells you how to connect to a private network using the VPN Client and an Internet connection; shows how to get status information on your connection, and how to use auto initiation.
Chapter 5	Managing the VPN Client	Tells you how to manage VPN Client connections, upgrade or uninstall VPN Client software, reconfigure the VPN Client automatically, use the Log Viewer application and set up special features such as Start Before Logon.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls:
Doc: 3701

Chapter	Title	Description
Chapter 6	Enrolling and Managing Certificates	Tells you how to obtain digital certificates to use for authentication and how to manage these certificates on your system.
Appendix A	Copyrights and Licenses	Provides copyright and license information for software that the VPN Client uses.

Terminology

In this user guide, the term Cisco VPN device refers to the following Cisco products:

- Cisco VPN 3000 Series Concentrator
- Cisco Secure PIX Firewall devices
- IOS platform devices, such as the Cisco 7100 Series Routers

Related documentation

The VPN Client includes an extensive online HTML-based help system that you can access through a browser in several ways:

- Click the Help icon on the Cisco Systems VPN Client programs menu (Start > Programs > Cisco Systems VPN Client > Help).
- Press **F1** while using the applications.
- Click the **Help** button on screens that include it.

The *VPN Client Administrator Guide* tells a network administrator how to:

- Configure a VPN 3000 Concentrator for several specific features:
  - Configure a VPN 3000 Concentrator for remote access users
  - Configure VPN Client firewall policy on a VPN 3000 Concentrator
  - Notify remote users of a client update
  - Set up Local LAN Access for the VPN Client
  - Configure the VPN Concentrator to update VPN Client backup servers
  - Set up the VPN Concentrator and the VPN Client for NAT Transparency
  - Configure Entrust Entelligence for the VPN Client
  - Set up authentication using Smart Cards.
- Automate remote user profiles
- Configure auto initiation
- Use the VPN Client command-line interface
- Customize the VPN Client software (text, icons and installation)
- Use the SetMTU application
- Obtain troubleshooting information
- Work with Microsoft Windows Installer

The VPN Client guides are provided on the Cisco VPN 3000 Concentrator's software distribution CD-ROM in PDF format. To view the latest version on the Cisco Web site, go to the following site and click **VPN Client**.

http://www.cisco.com/univercd/cc/td/doc/product/vpn/index.htm.

4.549
J

VPN 3000 Series Concentrator Documentation

The *VPN 3000 Concentrator Series Getting Started* guide explains how to unpack and install the VPN Concentrator, and how to configure the minimal parameters. This is known as *Quick Config*.

The *VPN 3000 Series Concentrator Reference Volume I: Configuration* explains how to start and use the VPN Concentrator Manager. It details the Configuration screens and explains how to configure your device beyond the minimal parameters you set during quick configuration.

The *VPN 3000 Series Concentrator Reference Volume II: Administration and Monitoring* provides guidelines for administering and monitoring the VPN Concentrator. It explains and defines all functions available in the Administration and Monitoring screens of the VPN Concentrator Manager. Appendixes to this manual provide troubleshooting guidance and explain how to access and use the alternate command-line interface.

The VPN Concentrator Manager also includes online help that you can access by clicking the **Help** icon on the toolbar in the Manager window.

Other useful books, articles, and websites include:

- *Dictionary of Internetworking Terms and Acronyms*. Cisco Press: 2001
- Kosiur, Dave. *Building and Managing Virtual Private Networks*. Wiley: 1998.
- Sheldon, Tom. *Encyclopedia of Networking*. Osborne/McGraw-Hill: 1998.
- `www.ietf.org` for Internet Engineering Task Force (IETF) Working Group drafts on IP Security Protocol (IPSec).

Conventions

This document uses the following conventions:

Convention	Description
boldface font	User actions and commands are in **boldface**.
italic font	Arguments for which you supply values are in *italics*.
`screen` font	Terminal sessions and information the system displays are in `screen` font.
`boldface screen` font	Information you must enter is in **`boldface screen`** font.

RQS Nº 03/2005 - CN -
CPMI - CORREIOS
Fls: 0952
Doc: 3701

Notes use the following conventions:

Note Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the publication.

Cautions use the following conventions:

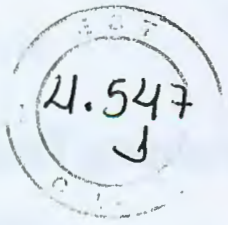
Caution Means *reader be careful*. Cautions alert you to actions or conditions that could result in equipment damage or loss of data.

Data Formats

As you configure and manage the system, enter data in the following formats unless the instructions indicate otherwise:

Type of Data	Format
IP Addresses	IP addresses use 4-byte dotted decimal notation (for example, `192.168.12.34`); as the example indicates, you can omit leading zeros in a byte position.
Subnet Masks and Wildcard Masks	Subnet masks use 4-byte dotted decimal notation (for example, `255.255.255.0`). Wildcard masks use the same notation (for example, `0.0.0.255`); as the example illustrates, you can omit leading zeros in a byte position.
MAC Addresses	MAC addresses use 6-byte hexadecimal notation (for example, `00.10.5A.1F.4F.07`).
Hostnames	Hostnames use legitimate network hostname or end-system name notation (for example, `VPN01`). Spaces are not allowed. A hostname must uniquely identify a specific system on a network.
Text Strings	Text strings use upper- and lower-case alphanumeric characters. Most text strings are case-sensitive (for example, simon and Simon represent different usernames). In most cases, the maximum length of text strings is 48 characters.
Port Numbers	Port numbers use decimal numbers from `0` to `65535`. No commas or spaces are permitted in a number.

Obtaining Documentation



These sections explain how to obtain documentation from Cisco Systems.

World Wide Web

You can access the most current Cisco documentation on the World Wide Web at this URL:

http://www.cisco.com

Translated documentation is available at this URL:

http://www.cisco.com/public/countries_languages.shtml

Documentation CD-ROM

Cisco documentation and additional literature are available in a Cisco Documentation CD-ROM package, which is shipped with your product. The Documentation CD-ROM is updated monthly and may be more current than printed documentation. The CD-ROM package is available as a single unit or through an annual subscription.

Ordering Documentation

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Networking Products MarketPlace:

  http://www.cisco.com/cgi-bin/order/order_root.pl

- Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:

  http://www.cisco.com/go/subscription

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, U.S.A.) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

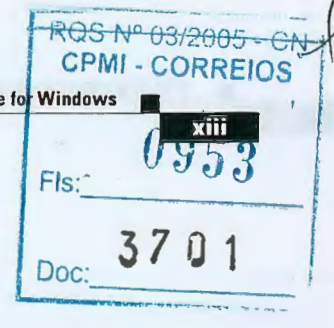
Documentation Feedback

You can submit comments electronically on Cisco.com. In the Cisco Documentation home page, click the **Fax** or **Email** option in the "Leave Feedback" section at the bottom of the page.

You can e-mail your comments to bug-doc@cisco.com.

You can submit your comments by mail by using the response card behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Document Resource Connection
170 West Tasman Drive
San Jose, CA 95134-9883



We appreciate your comments.

Obtaining Technical Assistance

Cisco provides Cisco.com as a starting point for all technical assistance. Customers and partners can obtain online documentation, troubleshooting tips, and sample configurations from online tools by using the Cisco Technical Assistance Center (TAC) Web Site. Cisco.com registered users have complete access to the technical support resources on the Cisco TAC Web Site.

Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world.

Cisco.com is a highly integrated Internet application and a powerful, easy-to-use tool that provides a broad range of features and services to help you with these tasks:

- Streamline business processes and improve productivity
- Resolve technical issues with online support
- Download and test software packages
- Order Cisco learning materials and merchandise
- Register for online skill assessment, training, and certification programs

If you want to obtain customized information and service, you can self-register on Cisco.com. To access Cisco.com, go to this URL:

http://www.cisco.com

Technical Assistance Center

The Cisco Technical Assistance Center (TAC) is available to all customers who need technical assistance with a Cisco product, technology, or solution. Two levels of support are available: the Cisco TAC Web Site and the Cisco TAC Escalation Center.

Cisco TAC inquiries are categorized according to the urgency of the issue:

- Priority level 4 (P4)—You need information or assistance concerning Cisco product capabilities, product installation, or basic product configuration.
- Priority level 3 (P3)—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- Priority level 2 (P2)—Your production network is severely degraded, affecting significant aspects of business operations. No workaround is available.
- Priority level 1 (P1)—Your production network is down, and a critical impact to business operations will occur if service is not restored quickly. No workaround is available.

The Cisco TAC resource that you choose is based on the priority of the problem and the conditions of service contracts, when applicable.

4.545
J

Cisco TAC Web Site

You can use the Cisco TAC Web Site to resolve P3 and P4 issues yourself, saving both cost and time. The site provides around-the-clock access to online tools, knowledge bases, and software. To access the Cisco TAC Web Site, go to this URL:

http://www.cisco.com/tac

All customers, partners, and resellers who have a valid Cisco service contract have complete access to the technical support resources on the Cisco TAC Web Site. The Cisco TAC Web Site requires a Cisco.com login ID and password. If you have a valid service contract but do not have a login ID or password, go to this URL to register:

http://www.cisco.com/register/

If you are a Cisco.com registered user, and you cannot resolve your technical issues by using the Cisco TAC Web Site, you can open a case online by using the TAC Case Open tool at this URL:

http://www.cisco.com/tac/caseopen

If you have Internet access, we recommend that you open P3 and P4 cases through the Cisco TAC Web Site.

Cisco TAC Escalation Center

The Cisco TAC Escalation Center addresses priority level 1 or priority level 2 issues. These classifications are assigned when severe network degradation significantly impacts business operations. When you contact the TAC Escalation Center with a P1 or P2 problem, a Cisco TAC engineer automatically opens a case.

To obtain a directory of toll-free Cisco TAC telephone numbers for your country, go to this URL:

http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml

Before calling, please check with your network operations center to determine the level of Cisco support services to which your company is entitled: for example, SMARTnet, SMARTnet Onsite, or Network Supported Accounts (NSA). When you call the center, please have available your service agreement number and your product serial number.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 0954
3701
Doc:

CHAPTER 1

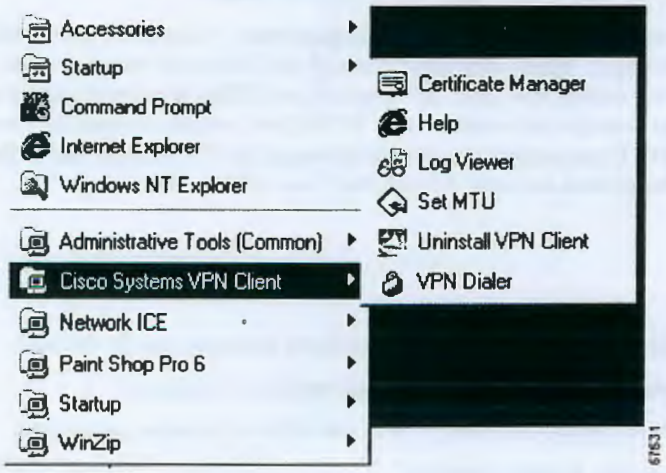
Understanding the Cisco VPN Client

The Cisco VPN Client for Windows (referred to in this user guide as *VPN Client*) is a software program that runs on a Microsoft® Windows®-based PC. The VPN Client on a remote PC, communicating with a Cisco Easy VPN server on an enterprise network or with a service provider, creates a secure connection over the Internet. Through this connection you can access a private network as if you were an on-site user. Thus you have a Virtual Private Network (VPN). The server verifies that incoming connections have up-to-date policies in place before establishing them. Cisco IOS, VPN 3000 Series Concentrators, and PIX central-site servers can all terminate VPN connections from VPN Clients.

As a remote user (low speed or high speed), you first connect to the Internet. Then you use the VPN Client to securely access private enterprise networks through a Cisco VPN server that supports the VPN Client.

The VPN Client comprises the following applications, which you select from the Programs menu:

Figure 1-1 VPN Client Applications as Installed by InstallShield



In logical order of use, the applications are as follows:

- Help—Displays an online manual with instructions on using the applications.
- VPN Dialer—Lets you configure connections to a VPN server and lets you then start your connections.
- Certificate Manager—Lets you enroll for certificates to authenticate your connections to VPN servers.
- Log Viewer—Lets you display events from the log.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 0955
Doc: 3701

- Uninstall VPN Client—Lets you safely remove the VPN Client software from your system and retain your connection and certificate configurations.

Note There are two ways to install the VPN Client: through the InstallShield wizard or through the Microsoft Installer. If you install the VPN Client through the Microsoft Installer, the Programs menu shown in Figure 1-1 does not contain the Uninstall application.

- SetMTU—Lets you manually change the size of the maximum transmission unit (see the *VPN Client Administrator Guide*, Chapter 6.)

How the VPN Client Works

The VPN Client works with a Cisco VPN server to create a secure connection, called a tunnel, between your computer and the private network. It uses Internet Key Exchange (IKE) and Internet Protocol Security (IPSec) tunneling protocols to make and manage the secure connection. Some of the steps include:

- Negotiating tunnel parameters—Addresses, algorithms, lifetime, and so on.
- Establishing tunnels according to the parameters.
- Authenticating users—Making sure users are who they say they are, by way of usernames, group names and passwords, and X.509 digital certificates.
- Establishing user access rights—Hours of access, connection time, allowed destinations, allowed protocols, and so on.
- Managing security keys for encryption and decryption.
- Authenticating, encrypting, and decrypting data through the tunnel.

For example, to use a remote PC to read e-mail at your organization, you connect to the Internet, then start the VPN Client and establish a secure connection through the Internet to your organization's private network. When you open your e-mail, the Cisco VPN server uses IPSec to encrypt the e-mail message. It then transmits the message through the tunnel to your VPN Client, which decrypts the message so you can read it on your remote PC. If you reply to the e-mail message, the VPN Client uses IPSec to process and return the message to the private network through the Cisco VPN server.

Connection Technologies

The VPN Client lets you use any of the following technologies to connect to the Internet:

- POTS (Plain Old Telephone Service)—Uses a dial-up modem to connect.
- ISDN (Integrated Services Digital Network)—May use a dial-up modem to connect.
- Cable—Uses a cable modem; always connected.
- DSL (Digital Subscriber Line)—Uses a DSL modem; always connected.

You can also use the VPN Client on a PC with a direct LAN connection.

4.541
J

VPN Client Features

The VPN Client includes the following features:

Program Features

- Complete browser-based context-sensitive HTML-based Help
- Support for VPN 3000 Series Concentrator platforms that run Release 3.0 and above. (VPN Client Release 3.0 and above will not work with Releases 2.x of the VPN 3000 Concentrator.)
- Command-line interface to the VPN Dialer
- Local LAN access—The ability to access resources on a local LAN while connected through a secure gateway to a central-site VPN server (if the central site grants permission)
- Automatic VPN Client configuration option—the ability to import a configuration file
- Log Viewer—An application that collects events for viewing and analysis
- Set MTU size—The VPN Client automatically sets a size that is optimal for your environment. However, you can set the MTU size manually as well. (For instructions on adjusting the MTU size, see the *VPN Client Administrator Guide).*
- Application Launcher—The ability to launch an application or a third-party dialer from the VPN Client.
- Automatic uninstall of the Nortel Networks VPN Client and the 5000 VPN Client software with the InstallShield installation package
- Automatic connection by way of Microsoft Dial-Up Networking or any other third-party remote access dialer
- Software update notifications from the VPN server upon connection
- Ability to launch a location site containing upgrade software from a VPN server notification
- The ability to automatically initiate secure wireless VPN connections seamlessly
- NAT Transparency (NAT-T), which lets the VPN Client and the VPN Concentrator automatically detect when to use IPSec over UDP to work properly in Port Address Translation environments.
- Update of centrally controlled backup server list—the VPN Client learns the backup VPN Concentrator list through connection establishment. This feature is configured on the VPN 3000 Concentrator and pushed to the VPN Client. The addresses show in the VPN Dialer application in the Enable Backup Servers box under Options->Properties->Connections.
- Support for Dynamic DNS (DDNS hostname population)—The VPN Client sends its hostname to the VPN Concentrator during connection establishment. The VPN Concentrator can send the hostname in a DHCP request that can cause a DNS server to update its database to include the new hostname and Client address.

Windows NT, Windows 2000, and Windows XP Features

- Password expiration information when authenticating through a RADIUS server that references an NT user database. When you log in, the VPN Concentrator sends a message that your password has expired and asks you to enter a new one and then confirm it. On pre-Release 3.5 VPN Clients, the prompt asks you to supply a PIN and to verify it. On a 3.5 or above VPN Client, the prompt asks you to enter and verify a password.

ROS Nº 03/2005 - CN
CPMI - 1-3 OS
Fls: 0956
Doc: 3701

- Start Before Logon—The ability to establish a VPN connection before logging on to a Windows NT platform, which includes Windows NT 4.0, Windows 2000, and Windows XP systems.
- Ability to disable automatic disconnect when logging off of a Windows NT platform. This allows for roaming profile synchronization.

IPSec Features

- IPSec tunneling protocol
- Transparent tunneling—IPSec over UDP for NAT and PAT, and IPSec over TCP for NAT, PAT, and firewalls
- IKE key management protocol
- IKE Keepalives—Monitoring the continued presence of a peer and reporting the VPN Client's continued presence to the peer. This lets the VPN Client notify you when the peer is no longer present. Another type of keepalives keeps NAT ports alive.
- Split tunneling—The ability to simultaneously direct packets over the Internet in clear text and encrypted through an IPSec tunnel. The VPN Server supplies a list of networks to the VPN Client for tunneled traffic. You enable split tunneling on the VPN Client and configure the network list on the VPN Server, such as the VPN Concentrator.
- Support for Split DNS—The ability to direct DNS packets in clear text over the Internet to domains served through an external DNS (serving your ISP) or through an IPSec tunnel to domains served by the corporate DNS. The VPN Server supplies a list of domains to the VPN Client for tunneling packets to destinations in the private network. For example, a query for a packet destined for *corporate.com* would go through the tunnel to the DNS that serves the private network, while a query for a packet destined for *myfavoritesearch.com* would be handled by the ISP's DNS. This feature is configured on the VPN Server (VPN Concentrator) and enabled on the VPN Client by default. To use Split DNS, you must also have split tunneling configured.
- LZS data compression, which can benefit modem users

Authentication Features

- User authentication by way of VPN central-site device:
  - Internal through the VPN device's database
  - RADIUS (Remote Authentication Dial-In User Service)
  - NT Domain (Windows NT)
  - RSA (formerly SDI) SecurID or SoftID
- Certificate Manager—An application that lets you manage your identity certificates
- Ability to use Entrust Entelligence certificates
- Ability to authenticate using smart cards with certificates
- Peer Certificate Domain Name Verification—prevents a client from connecting to a invalid gateway by using a stolen but valid certificate and a hijacked IP address. If the attempt to verify the domain name of the peer certificate fails, the client connection also fails.

4.539
J

Firewall Features

- Support for Cisco Secure PIX Firewall platforms that run Release 6.0 and higher

Note Instructions on configuring the VPN Client to interoperate with Cisco Secure PIX Firewall, Release 6.0 and above, are available in *IPSec User Guide for Cisco Secure PIX Firewall.*

- Support for personal firewalls:
  - Cisco Integrated Firewall (CIC)
  - ZoneAlarmPro 2.6.3.57
  - ZoneAlarm 2.6.3.57
  - Zone Integrity
  - BlackIce Agent and BlackIce Defender 2.5
- Centralized Protection Policy—Support for firewall policies pushed to the VPN Client from a VPN Concentrator

VPN Client IPSec Attributes

The VPN Client supports these IPSec attributes:

- Main mode for negotiating phase one of establishing ISAKMP Security Associations (SAs)
- Aggressive mode for negotiating phase one of establishing ISAKMP SAs
- Authentication algorithms:
  - HMAC (Hashed Message Authentication Coding) with MD5 (Message Digest 5) hash function
  - HMAC with SHA-1 (Secure Hash Algorithm) hash function
- Authentication Modes:
  - Preshared Keys
  - X.509 Digital Certificates
- Diffie-Hellman Groups 1(for digital certificates), 2, and 5
- Encryption algorithms:
  - 56-bit DES (Data Encryption Standard)
  - 168-bit Triple-DES
  - AES 128-bit and 256-bit

Note You must be running Release 3.6 of the VPN Client to use the AES encryption algorithm

- Extended Authentication (XAUTH)
- Mode Configuration (also known as ISAKMP Configuration Method)
- Tunnel Encapsulation Mode
- IP compression (IPCOMP) using LZS

ROS Nº 03/2005 - CN
CPMI - 1-5 IOS
0957
Fls:
3701
Doc:

4.537

CHAPTER 2

Installing the VPN Client

This chapter explains how to install the VPN Client on your PC and includes the following sections:

- Verifying System Requirements
- Gathering Information You Need
- Installing the VPN Client Through InstallShield
- Installing the VPN Client Through Microsoft Windows Installer

To upgrade the VPN Client software, or to uninstall it, see "Managing the VPN Client."

Caution Installing the VPN Client software using InstallShield on Windows NT or Windows 2000 requires Administrator privileges. If you do not have Administrator privileges, you must have someone with Administrator privileges install the product for you.

Installation Applications

You can install the VPN Client on your system through two different applications: InstallShield and Microsoft Windows Installer (MSI). Both applications use installation wizards to walk you through the installation. Installing the VPN Client through InstallShield includes an Uninstall icon in the program group; MSI does not. In the latter case, to manually remove VPN Client applications, you can use the Microsoft Add/Remove Programs utility.

Verifying System Requirements

Verify that your computer meets these requirements:

- Computer with a Pentium®-class processor or greater
- One of the following operating systems:
  - Microsoft®Windows® 95 (OSR2), Windows 98, or Windows 98 (second edition)
  - Windows ME
  - Windows NT® 4.0 (with Service Pack 6, or higher)
  - Windows 2000
  - Windows XP

POS Nº 03/2005 - CN
CPMI - [redacted] OS
0958
Fls:
Doc:
3701

- Microsoft TCP/IP installed. (Confirm via Start > Settings > Control Panel > Network > Protocols or Configuration.)
- 10 MB hard disk space.
- RAM:
  - 16 MB for Windows 95/98
  - 32 MB for Windows NT and Windows ME
  - 64 MB for Windows 2000
  - 128 MB for Windows XP
- To install the VPN Client:
  - CD-ROM drive
  - 3.5 inch high-density diskette drive
  - Administrator privileges if installing on Windows NT or Windows 2000
- To use the VPN Client:
  - Direct network connection (cable or DSL modem and network adapter/interface card)
  - Internal or external modem
  - For Windows 95, Microsoft Dial-Up Networking (DUN) version 1.2 or greater. (DUN 1.3 for Windows 95 is a recommended performance and security upgrade, and it is available as a free download from the Microsoft Web site, www.microsoft.com. Windows 98 includes the DUN 1.3 functionality.)
- To connect using a digital certificate for authentication:
  - A digital certificate signed by one of the following Certificate Authorities (CAs) installed on your PC:

    Baltimore Technologies (www.baltimoretechnologies.com)

    Entrust Technologies (www.entrust.com)

    Microsoft Certificate Services—Windows 2000

    Netscape (Security)

    Verisign, Inc. (www.verisign.com)
  - Or a digital certificate stored on a smart card. The VPN Client supports smart cards via the MS CAPI Interface.

Gathering Information You Need

To configure and use the VPN Client, you may need the information listed in this section.

Ask for this information from the system administrator of the private network you want to access. Your system administrator may have preconfigured much of this data; if so, he or she will tell you which items you need.

- Hostname or IP address of the secure gateway to which you are connecting
- Your IPSec Group Name (for preshared keys)
- Your IPSec Group Password (for preshared keys)
- If authenticating with a digital certificate, the name of the certificate

14.535

- If authenticating through the secure gateway's internal server, your username and password
- If authenticating through a RADIUS server, your username and password
- If authenticating through an NT Domain server, your username and password
- If authenticating through a token vendor, your username and PIN
- If authenticating through a smart card, your smart card, reader, PIN or passcode, and the name of the certificate stored on the smart card
- If you should configure backup server connections, the hostnames or IP addresses of the backup servers

Installing the VPN Client Through InstallShield

To install the VPN Client on your system, follow these steps. We suggest you accept the defaults unless your system administrator has instructed otherwise.

Step 1 Exit all Windows programs, and disable any antivirus software.

Step 2 Insert the Cisco Systems CD-ROM in your system's CD-ROM drive.

Step 3 Choose **Start > Run**. The Run dialog box appears.

Step 4 Enter E:\VPN Client\CD-ROM\InstallShield\setup.exe, where E: is your system's CD-ROM drive.

Step 5 Click **OK**.

Note Cisco does not allow you to install the VPN Client software from a network drive. If you attempt to do so, you receive an error message.

The program displays the Cisco Systems logo and InstallShield Setup window shown in Figure 2-1.

ROS Nº 03/2005 - CN
CPMI - 2-3 OS
Fls: 0959
Doc: 3701

Figure 2-1 Starting InstallShield Installation

Step 6 If the InstallShield Wizard identifies an existing version of the VPN Client, the Cisco 5000 Client, or Nortel Networks Extranet Access Client, it displays a dialog box that asks if you want to uninstall the existing client program. To continue, choose **Yes**.

The VPN Client launches the appropriate uninstall wizard: the Cisco VPN Client uninstall wizard to uninstall a previous version of the VPN Client, the Extranet Access Client wizard program, or the Cisco 5000 wizard. Follow the instructions on the uninstall wizard dialog boxes to automatically uninstall the program and reboot.

Note Having more than one VPN client on your system is not advisable.

After your system reboots, our own Cisco Systems VPN Client Setup wizard resumes.

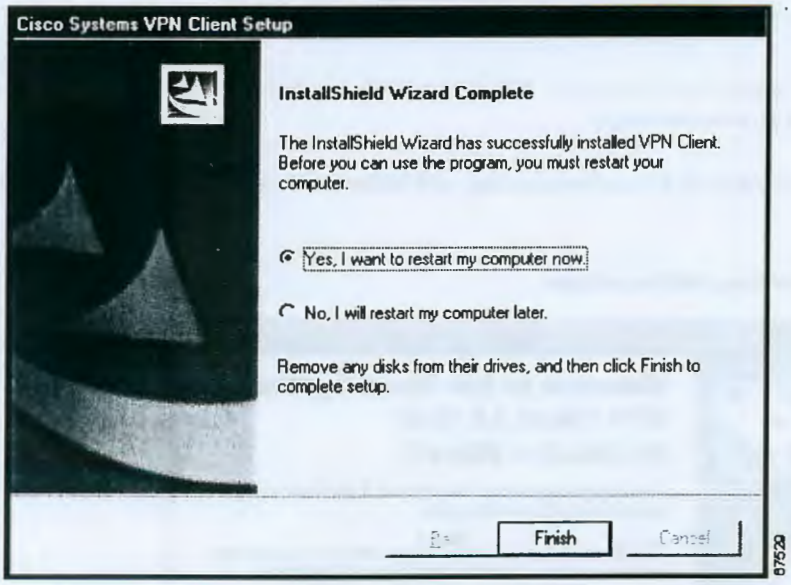
Step 7 Follow the instructions on the screens and enter the following information:

A destination folder for the VPN Client files (or click **Next>** to enter the default location C:\Program Files\Cisco Systems\VPN Client).

Step 8 After you have installed the VPN Client, the InstallShield Wizard displays the following screen. You must restart your computer before you can configure and use the VPN Client. (See Figure 2-2.)

4.533
S

Figure 2-2 Completing InstallShield Installation



- To restart now, click **Finish**. Your system reboots. *Be sure to remove any diskette from the drive before you reboot.*
- To restart later, click the **No** radio button and then click **Finish**. The VPN Client Setup closes. Remember: *you must restart your computer before you can use the VPN Client.*

Installing the VPN Client Through Microsoft Windows Installer

Microsoft Windows Installer (MSI) is available for Windows NT, Windows 2000, and Windows XP. To install the VPN Client using MSI, use the following procedure.

Step 1 Exit all Windows programs, and disable any antivirus software.

Step 2 Remove any VPN client software currently on your system including the following applications:

- IRE/SafeNet Client
- Nortel Networks VPN Client
- Altiga VPN Client
- Cisco VPN 3000 Client
- Cisco VPN 5000 Client
- Cisco VPN Client v3.0 through v3.6

To remove these applications, select **Control Panel > Add/Remove Programs**. Select the application and then click **Add/Remove**. After Windows removes the application, you must reboot your system.

Step 3 Insert the Cisco Systems CD-ROM in your system's CD-ROM drive.

Step 4 Choose **Start > Run**. The Run dialog box appears.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls: 0960
3701
Doc:

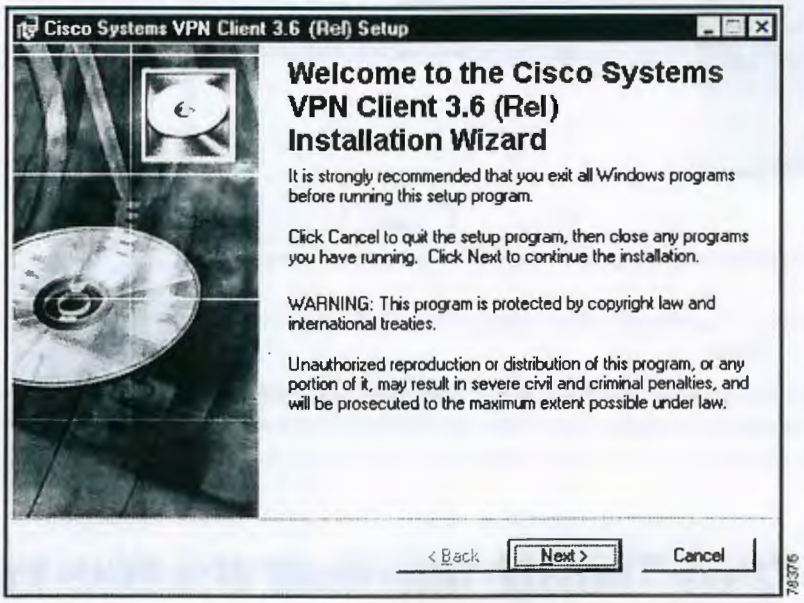
Step 5 Enter E:\VPN Client\CD-ROM\Msi\vpclient_en.exe, where E: is your system's CD-ROM drive.

Step 6 Click **OK**.

Note Cisco does not allow you to install the VPN Client software from a network drive. If you attempt to do so, you receive an error message.

The program displays the Cisco Systems logo and Microsoft Installer Setup window shown in Figure 2-3.

Figure 2-3 Starting MSI Installation

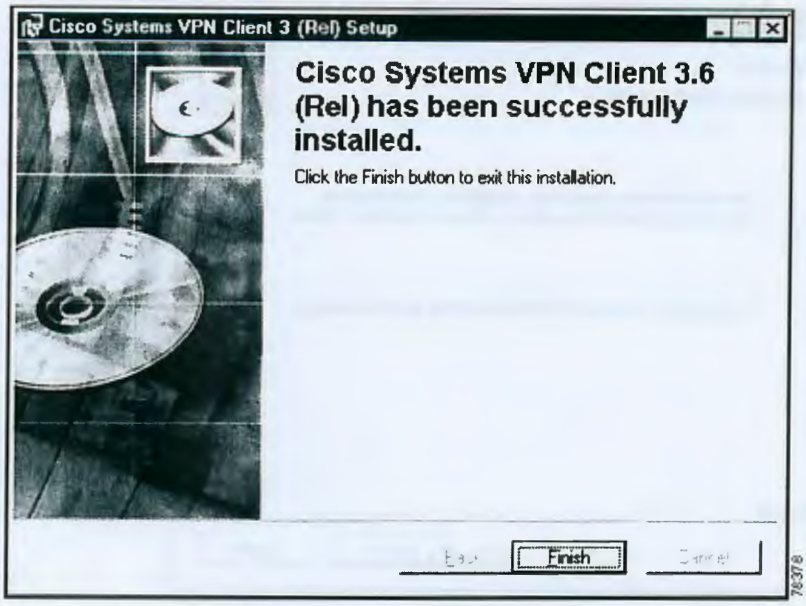


Step 7 Click **Next** to start the installation and then follow the instructions on the dialogs.

MSI installs the VPN Client in the default location C:\Program Files\Cisco Systems\VPN Client. If you want a different destination folder for the VPN Client files, enter the alternative location when prompted to do so.

When the installation has been completed, the installer displays the dialog in Figure 2-4.

Figure 2-4 Completing MSI Installation



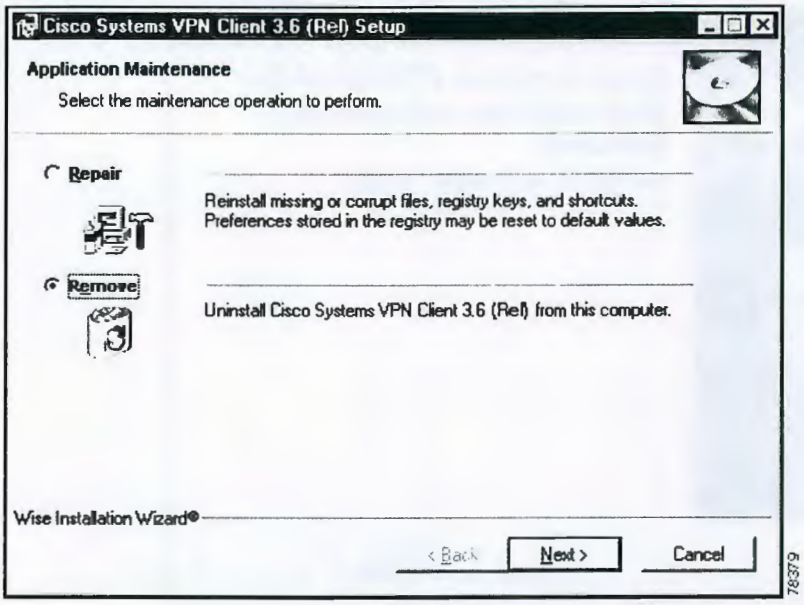
Step 8 Click **Finish**. MSI prompts you to restart your system.

Step 9 Click **Yes** to restart your system.

Note If you have not removed the VPN Client 3.6, when you execute the vpnclient_en.exe command or vpnclien_en.msi, a maintenance and repair wizard displays. See Figure 2-5. You do not see these screens when you remove the software through the Add/Remove programs utility.

4.531
RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 0961
3701
Doc:

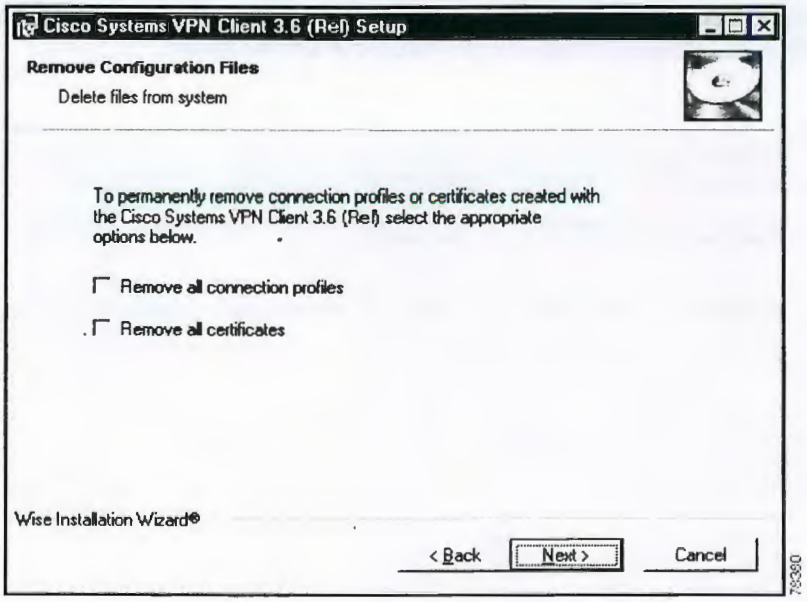
Figure 2-5 Repairing/Removing VPN Client Applications



To remove the VPN Client version 3.6 from your system, follow these steps:

Step 1 Click the **Remove** radio button and then click **Next**. The maintenance wizard displays the Remove Configuration Files dialog. (See Figure 2-6)

Figure 2-6 Removing Cisco VPN Client 3.6

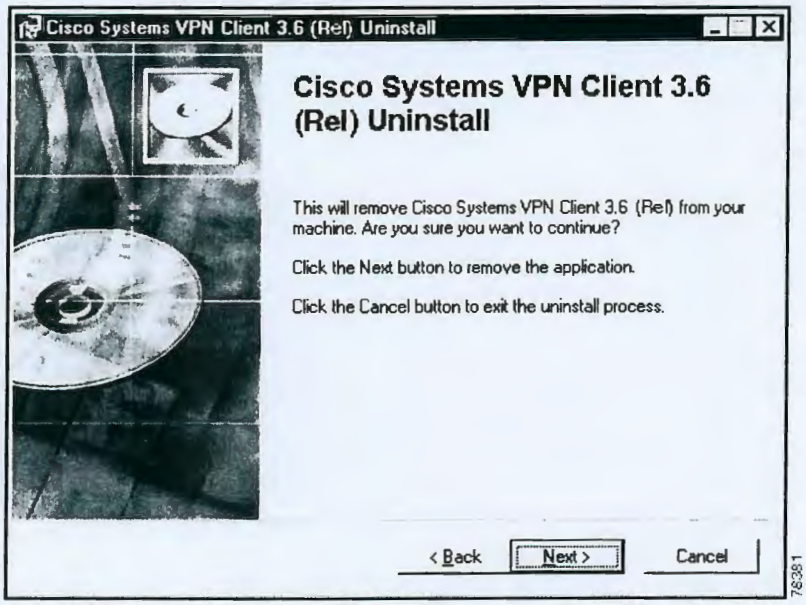


Step 2 If you want to remove your connection profiles and/or certificates, click the box(es) on the dialog. By default, this wizard does not delete these files. To continue, press **Next.** .

The wizard continues and displays the dialog shown in Figure 2-7.

21.529
J

Figure 2-7 Cisco Systems VPN Client 3.6 Uninstall dialog



Step 3 To remove the Cisco VPN Client version 3.6, click **Next**. Or to halt the wizard, click **Cancel**.

When you click Next, the wizard removes the Cisco VPN Client version 3.6. If you elected to remove your connection profiles and/or certificates, these files are also removed; otherwise, these files remain on your system.

When you click Cancel, the wizard prompts you to either Resume or Exit Setup. To stop removal, click **Exit Setup**. If you want to continue the removal, click **Resume**.

What Next?

When the VPN Client software is installed on your PC, to configure it, see "Configuring the VPN Client."

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 0962
3701
Doc:

CHAPTER 3

Configuring the VPN Client

This chapter explains how to configure the VPN Client.

To configure the VPN Client, you enter values for a set of parameters known as a *connection entry*. The VPN Client uses a connection entry to identify and connect securely to a specific private network.

Parameters include a name and description for the connection, the name or address of the VPN device (remote server), and information that identifies you to the VPN device.

Note If your system administrator has completely configured your connection entry for you, you can skip this chapter and go directly to "Connecting to a Private Network."

This chapter explains the following configuration tasks:

- How to Get Help
- What Is a Connection Entry?
- How To Create a New Connection Entry
- Setting or Changing Connection Entry Properties
- Changing the VPN Device Address for a Connection Entry

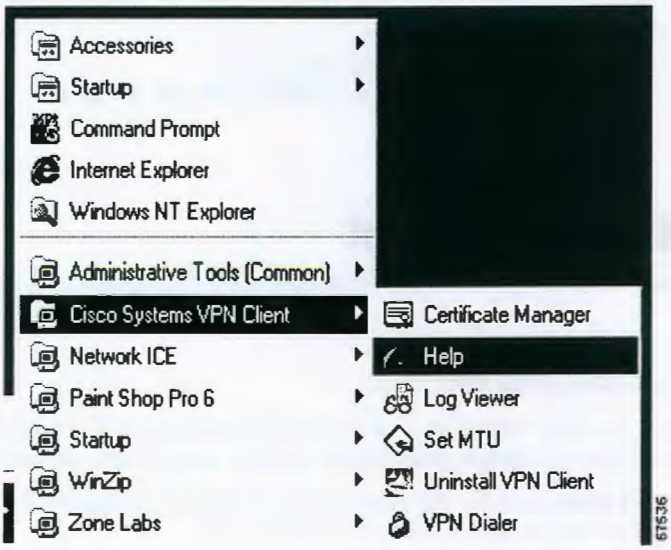
How to Get Help

The VPN Client comes with a complete, context-sensitive, browser-based help system. You can display help in the following ways:

- On the Program Menu, choose **Start > Programs > Cisco Systems VPN Client > Help.** (See Figure 3-1.) This method displays the entire help file beginning with a list of topics.

RDS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 0963
Doc:

Figure 3-1 Choosing Help from the Cisco Systems VPN Client Program Menu

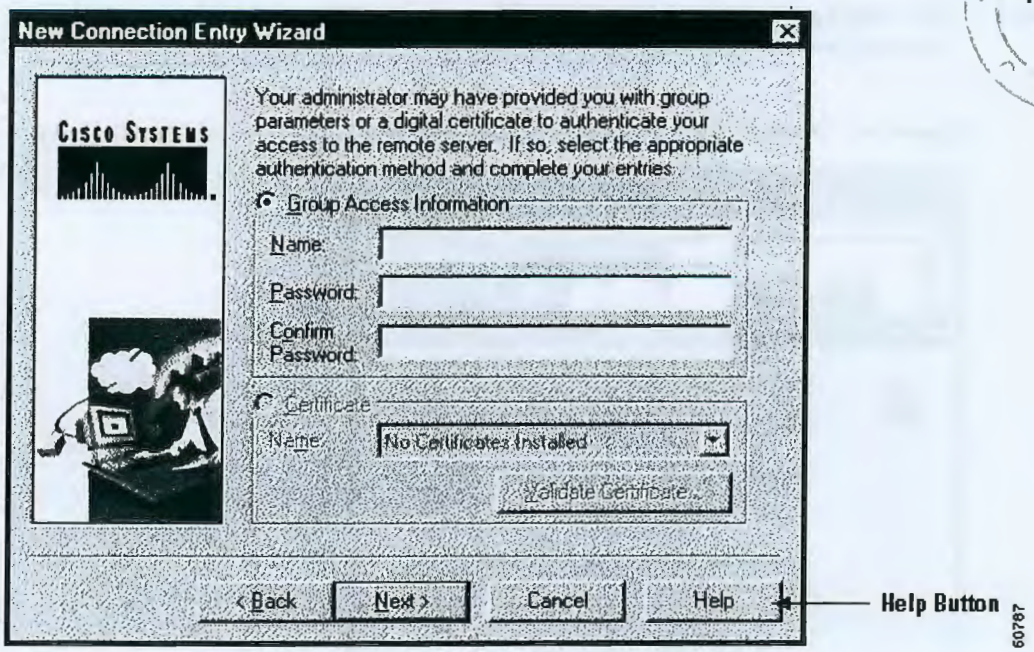


Note If you installed the VPN Client via the Microsoft Windows Installer, the Cisco Systems VPN Client menu does not include the Uninstall VPN Client option.

- Press **F1** at any window while using the VPN Client, including the main window of each application (VPN Dialer, Log Viewer, and Certificate Manager). This method displays context-sensitive information.
- Click the **Help** button on windows that display it. (See Figure 3-2.) This method displays context-sensitive information.

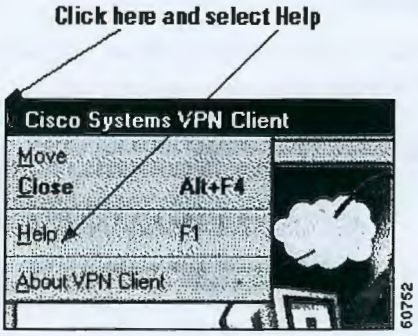
4.525
J

Figure 3-2 Help Button



- Choose **Help** from the menu that appears when you click on the icon in the title bar. (See Figure 3-3.)

Figure 3-3 Menu Containing Help Option



Determining the VPN Client Version

To display the version number of the software release you are currently using, follow these steps:

Step 1 Click the icon in the title bar. (See Figure 3-3.)

The VPN Client displays a menu.

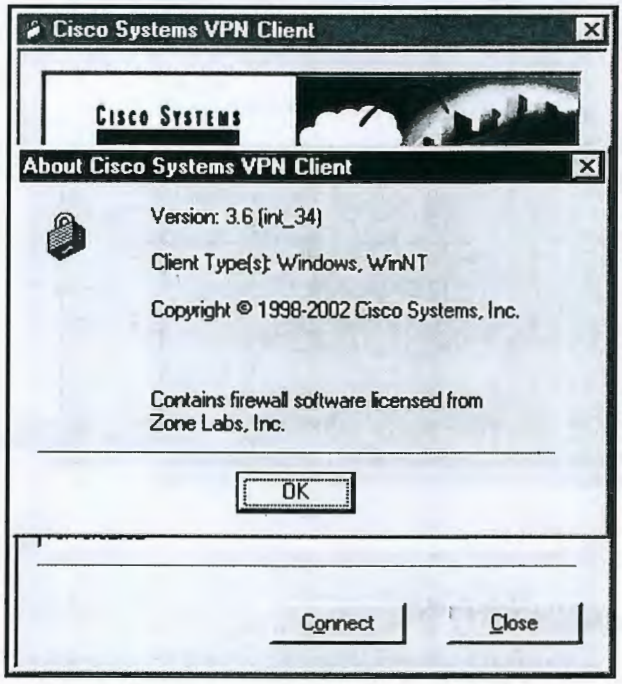
Step 2 Click **About VPN Client** on the menu displayed.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0304
Fls:
3701
Doc:

The VPN Client displays the version you are currently using. (See Figure 3-4.)

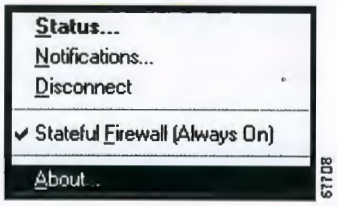
Step 3 After viewing the version number, click **OK**.

Figure 3-4 Displaying the VPN Client Software Version



When you are connected, you can display the software version by clicking **About...** on the menu you display by right clicking the Dialer icon in the system tray.

Figure 3-5 Displaying Version from Menu Available from System Tray



What Is a Connection Entry?

To use the VPN Client, you must create at least one connection entry, which identifies the following information:

- The VPN device (the remote server) to access
- Preshared keys—The IPSec group to which the system administrator assigned you. Your group determines how you access and use the remote network. For example, it specifies access hours, number of simultaneous logins, user authentication method, and the IPSec algorithms your VPN Client uses
- Certificates—The name of the certificate you are using for authentication
- Optional parameters that govern VPN Client operation and connection to the remote network

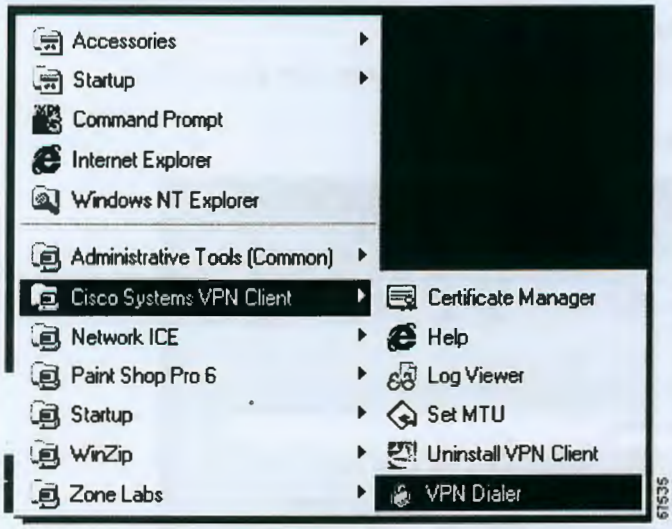
You can create multiple connection entries if you use your VPN Client to connect to multiple networks (though not simultaneously) or if you belong to more than one VPN remote access group.

For connection entry parameters, see "Gathering Information You Need".

How To Create a New Connection Entry

Start the VPN Client by choosing **Start > Programs > Cisco Systems VPN Client > VPN Dialer**.

Figure 3-6 Starting the VPN Dialer

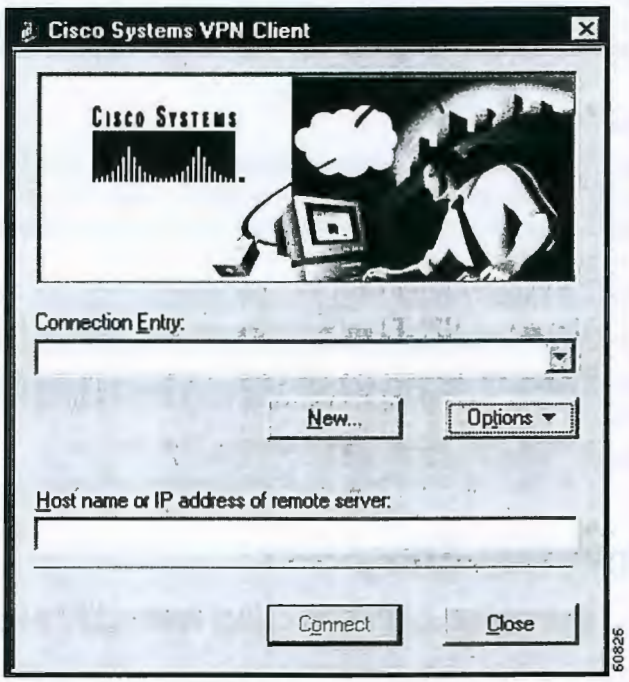


Note If you installed the VPN Client via the Microsoft Windows Installer, the Cisco Systems VPN Client menu does not include the Uninstall VPN Client option.

The VPN Dialer application starts and displays its main dialog box. (See Figure 3-7.)

4.523
CPMI 3-5 EIOS
Fls: 0965
3701
Doc:

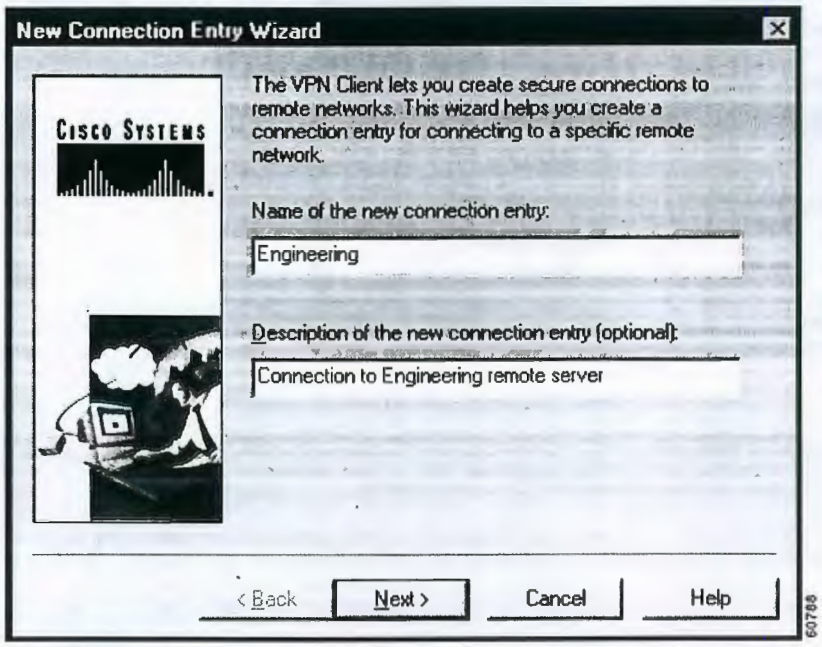
Figure 3-7 VPN Dialer Main Dialog Box



Step 1 At the main dialog, click **New**.

The first New Connection Entry Wizard dialog box appears. (See Figure 3-8.)

Figure 3-8 Entering Name and Description



4.521

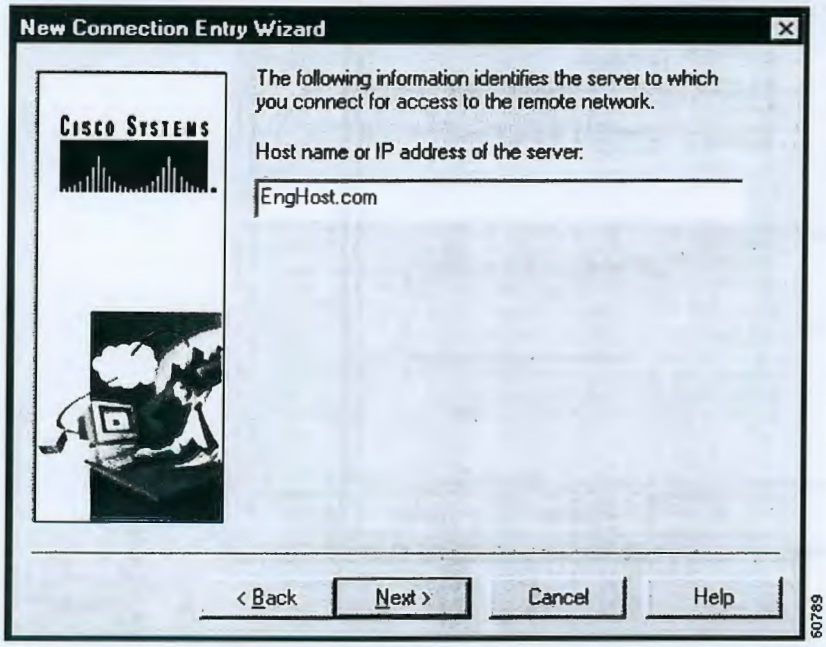
Step 2 Enter a unique name for this new connection. You can use any name to identify this connection, for example, Engineering. This name can contain spaces, and it is not case-sensitive.

Step 3 Enter a description of this connection. This field is optional, but it helps further identify this connection. For example, Connection to Engineering remote server.

Step 4 Click **Next**.

The second New Connection Entry Wizard dialog box appears. (See Figure 3-9.)

Figure 3-9 Identifying Server



Step 5 Enter the hostname or IP address of the remote VPN device you want to access, and click **Next**.

The third New Connection Entry Wizard dialog box appears. (See Figure 3-10.)

hoosing an Authentication Method

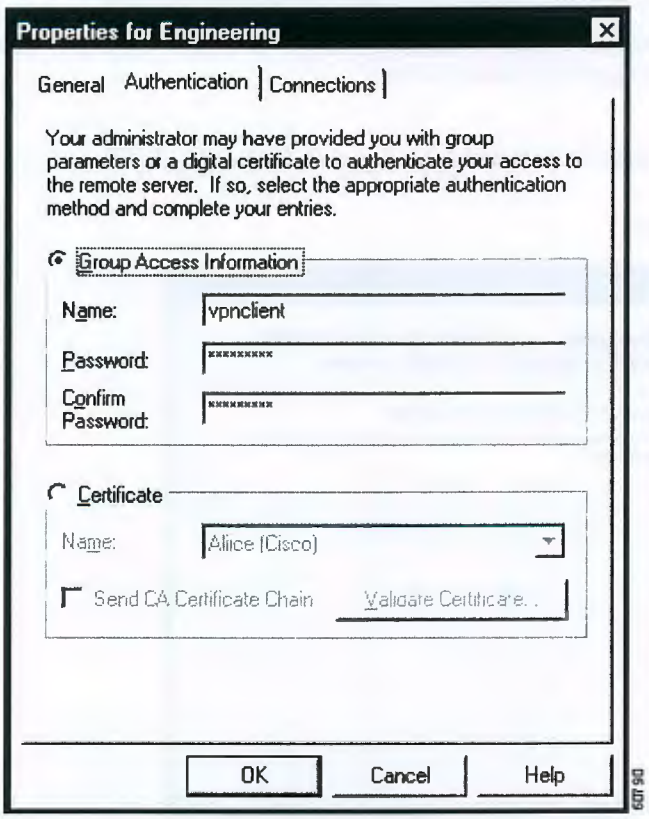
You can connect as part of a group (configured on a VPN device) or by supplying an identity digital certificate.

Group Authentication

For group authentication, perform the following procedure: (See Figure 3-10.)

CPMI - CORREIOS
0966
Fls: 3701
Doc:

Figure 3-10 Group Authentication



Step 1 In the Name field, enter the name of the IPSec group to which you belong. This entry is case-sensitive.

Step 2 In the Password field, enter the password (which is also case-sensitive) for your IPSec group. The field displays only asterisks.

Step 3 Verify your password by entering it again in the Confirm Password field.

Step 4 To continue, click **Next**.

Certificate Authentication

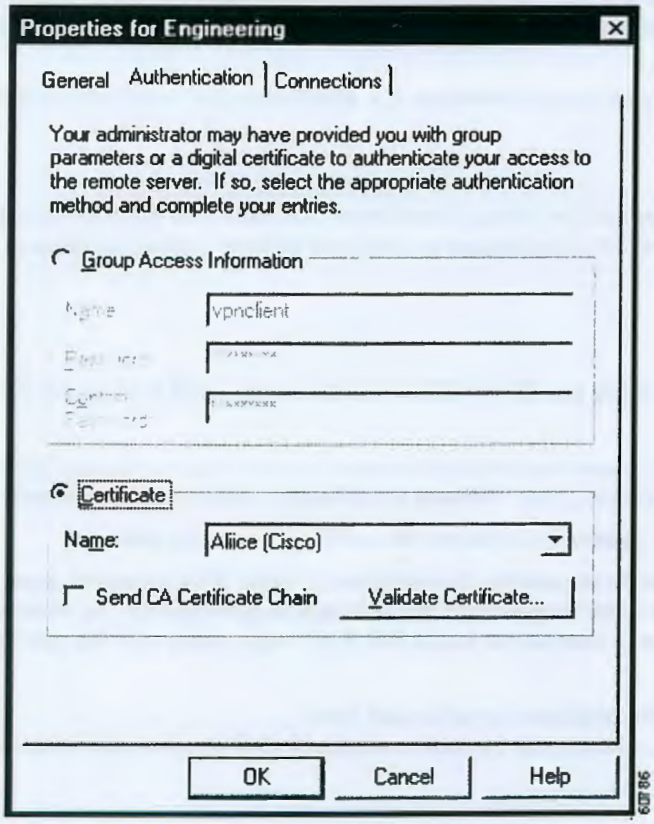
For certificate authentication, perform the following procedure, which varies according the type of certificate you are using:

Step 1 Click the **Certificates** radio button.

Step 2 Choose the name of the certificate you are using from the pull-down menu. (See Figure 3-11.)

If the field says No Certificates Installed and is shaded, then you must first enroll for a certificate before you can use this feature. For information on enrolling for a certificate, see "Enrolling and Managing Certificates" Or, consult your network administrator.

Figure 3-11 Certificate Authentication



Sending a Certificate Authority Certificate Chain

To send CA certificate chains, click **Send CA Certificate Chain**. This parameter is disabled by default.

The CA certificate chain includes all CA certificates in the hierarchy of certificates from the root certificate, which must be installed on the VPN Client, to the identity certificate. This feature enables the a peer VPN Concentrator to trust the VPN Client's identity certificate given the same root certificate, without having all the same subordinate CA certificates actually installed.

Example 3-1 CA Certificate Chains

1. On the VPN Client, you have this chain in the certificate hierarchy:
   - Root Certificate
   - CA Certificate 1
   - CA Certificate 2

EROS Nº 03/2005 - CN
CPM 3-9 REIOS
Fls: 0967
3701
Doc:

- Identity Certificate

2. On the VPN Concentrator, you have this chain in the certificate hierarchy
   - Root Certificate
   - CA Certificate 3
   - Identity Certificate
3. Though the identity certificates are issued by different CA certificates, the VPN Concentrator can still trust the VPN Client's identity certificate, since it has received the chain of certificates installed on the VPN Client PC.

This feature provides flexibility since the intermediate CA certificates don't need to be actually installed on the peer.

Note Certificate chains are not supported for Entrust Entelligence. Therefore the Send CA Certificate Chain checkbox on the Authentication Tab is unchecked and disabled when you select Entelligence Certificate.

Validating a Certificate

Optionally you might want to verify that the certificate you are using is still valid, using the following procedure:

Step 1 To verify the validity of a certificate, click **Validate Certificate...** and enter the password.

If the VPN Dialer prompts for a password to secure the certificate, enter the password.

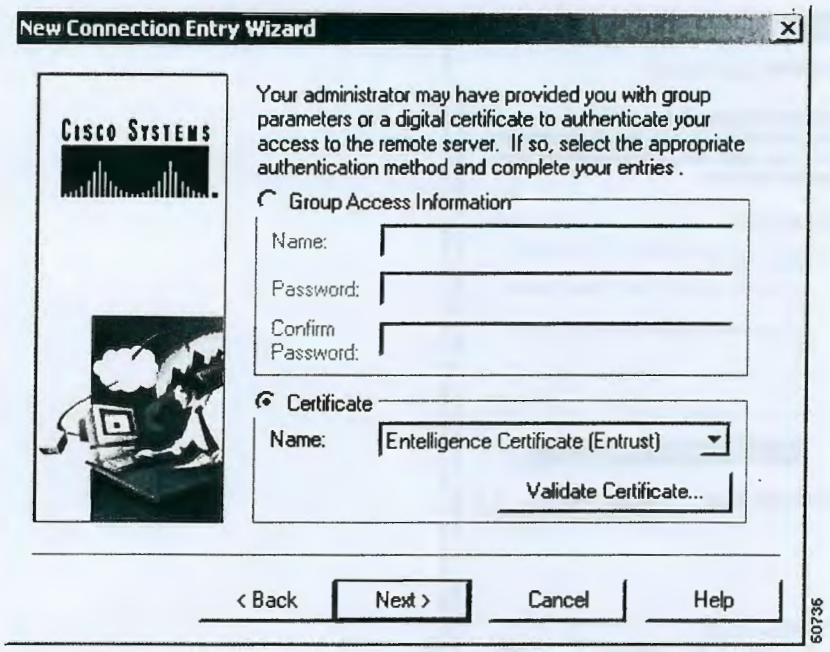
You receive a report letting you know whether the certificate is valid. If the password is not valid, you need to try again. If you do not know the password, see your system administrator. An identity certificate has a public and private key, and a time period within which it is valid. Make sure the certificate is valid before you continue.

Step 2 After you have verified that the certificate is valid, click **Next**.

Configuring an Entrust Certificate for Authentication

If you have an Entrust Entelligence certificate enrolled, the pull-down menu includes the entry "Entelligence Certificate (Entrust)." (See Figure 3-12.)

Figure 3-12 Entrust Entelligence Certificate



An Entrust Entelligence certificate is stored in a *Profile*, which you obtain when you log in to Entrust Entelligence.

Choose **Entelligence Certificate (Entrust)** from the pull-down menu and click **Next**.

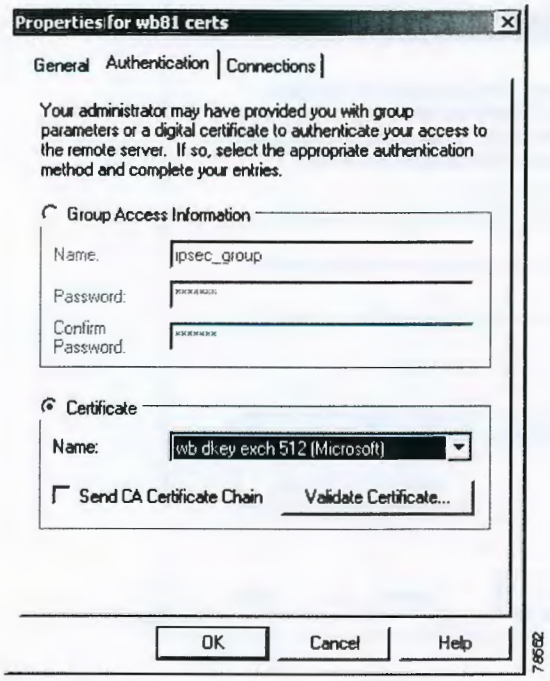
For more information about connecting with Entrust Entelligence, see "Connecting with an Entrust Certificate."

Configuring a Connection Entry for a Smart Card

If you are using a smart card or electronic token to authenticate a connection, create a connection entry that defines the certificate provided by the smart card. For example, if you are using ActivCard Gold, an accompanying certificate is in the Microsoft Certificate Store. When you create a new connection entry for using the smart card, select that certificate. (See Figure 3-13.)

4.517
RQS Nº 03/2005 - C...
CPMI - CORREIOS
3-11
0968
Fls:
3701
Doc:

Figure 3-13 Creating a Connection Entry for a Smart Card



Smart Cards Supported

The VPN Client supports authentication with digital certificates through a smart card or an electronic token. There are several vendors that provide smart cards and tokens, including the following:

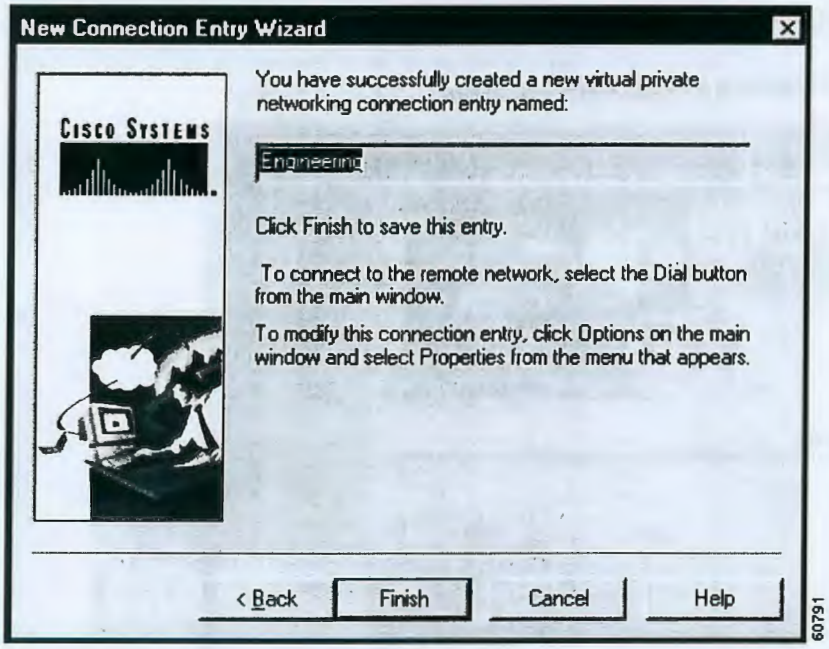
Vendor	Software and Version	Card/Token Tested	Vendor Web site
GemPLUS	GemSAFE Workstation 2.0 or later	GEM195	www.gemplus.com
Activcard	Activcard Gold version 2.0.1 or later	Palmera 32K	www.activcard.com
Aladdin	eToken Runtime Environment (RTE) version 2.6 or later	PRO and R2 tokens	www.ealaddin.com

The VPN Client works only with smart cards and tokens that support CRYPT_NOHASHOID.

Completing the Connection Wizard

After you enter authentication information and click **Next**, the fourth New Connection Entry Wizard dialog box appears. (See Figure 3-14.)

Figure 3-14 Completing the Connection Entry



To complete the connection entry configuration, use the following procedure.

Step 1 Review the connection entry name. If you want to change any previous entries, click **Back** until you get to the desired dialog box.

Step 2 To complete your entry, click **Finish**.

The final New Connection Entry Wizard dialog box closes. Your new connection entry now appears in the Connection Entry drop-down list on the VPN Client's main dialog box.

What Next?

If you need to configure optional connection entry parameters or change parameters for an existing connection entry, continue to the next section.

Otherwise, you can skip to "*Connecting to a Private Network.*"

4.515
RQS Nº 03/2005 - CN
CPMI CORREIOS
3-13
0969
Fls:
3701
Doc:

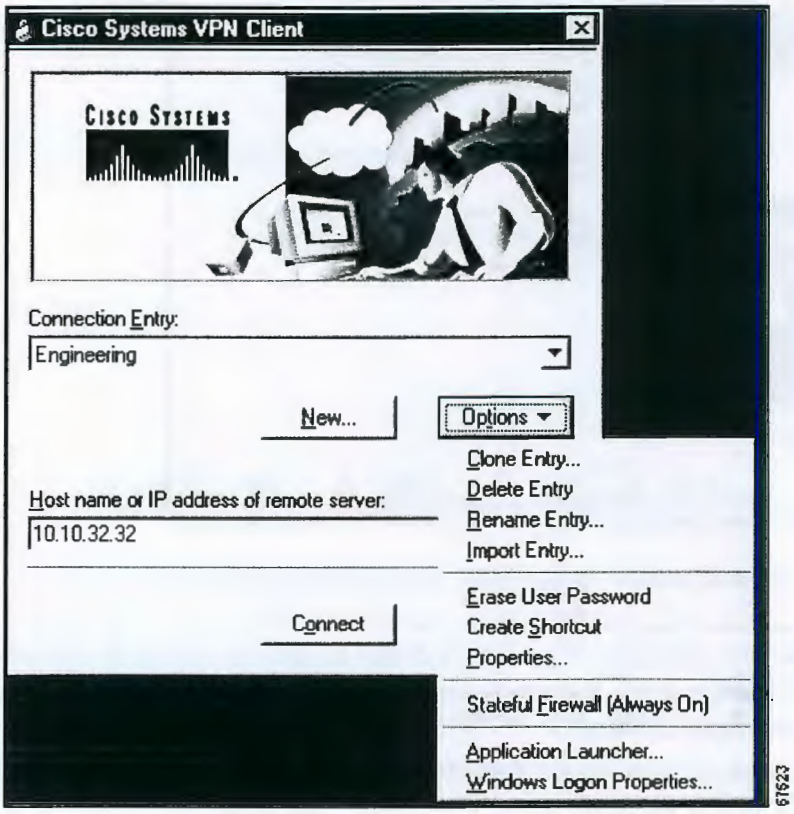
Setting or Changing Connection Entry Properties

To change parameters or to set optional parameters for an existing connection entry, follow these steps:

Step 1 In the VPN Client's main dialog box, click the Connection Entry drop-down menu button and choose the entry you want to configure.

Step 2 Then click **Options** and choose **Properties** from the menu. (See Figure 3-15.)

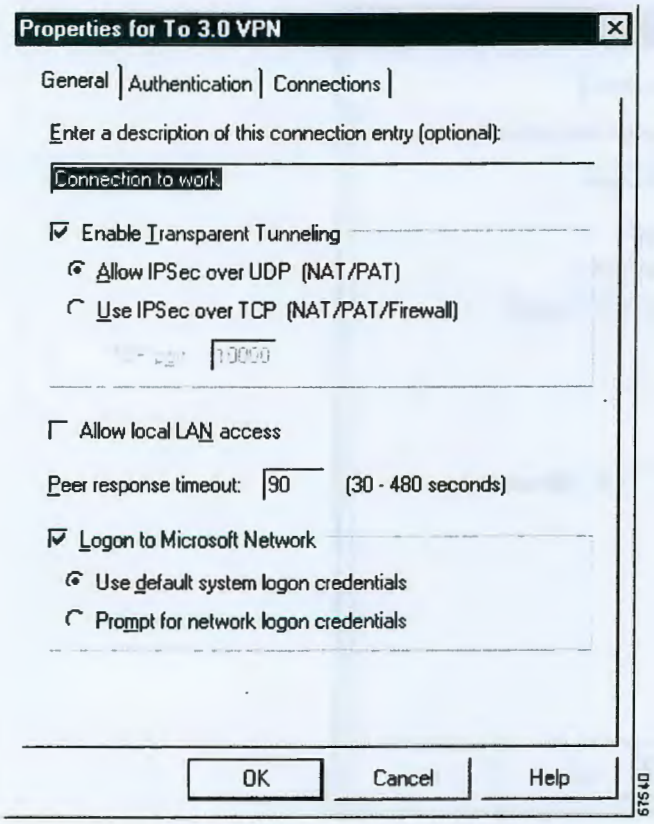
Figure 3-15 VPN Client Options Menu



The Properties dialog box appears. The fields in this dialog box differ according to the operating system you are using.

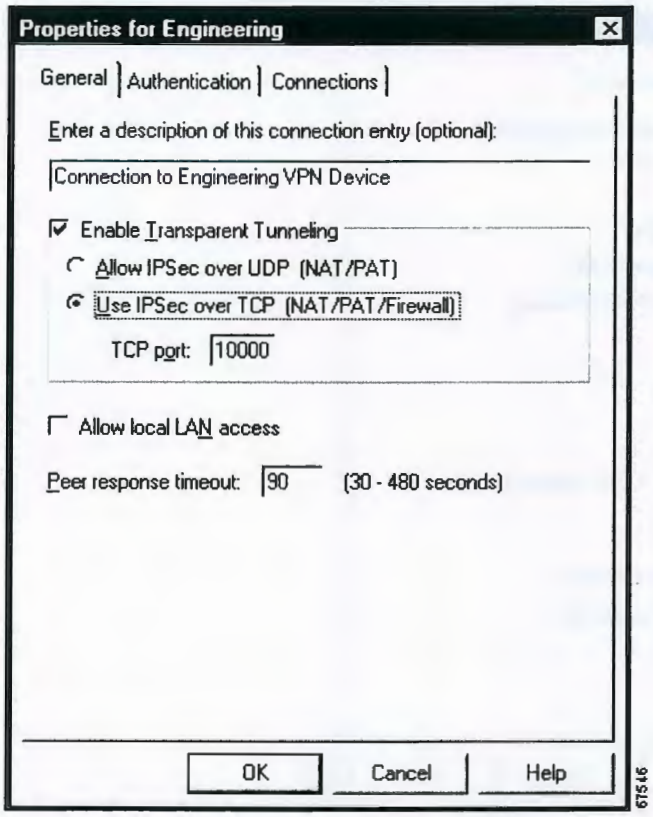
- If you are using Microsoft Windows 95, Windows 98, or Windows ME, you see a dialog box that resembles the one in Figure 3-16.
- If you are using Microsoft Windows NT, Windows 2000, or Windows XP, you see the dialog box in Figure 3-17.

Figure 3-16 Connection Entry Properties Dialog Box (Windows 95, Windows 98 and Windows ME)



4.513
RQS Nº 03/2005 - CN
CPMI - CORREIOS
3-15
0970
Fls:
3701
Doc:

Figure 3-17 Connection Entry Properties Dialog Box (Windows NT, Windows 2000, and Windows XP)



Step 3 Click the tab for the parameters you want to change:

- General tab
  - Change the connection entry description
  - Enable transparent tunneling
  - Allow local LAN Access
  - Adjust the peer response time out
  - Log on to Microsoft Network
- Authentication tab
  - Change the group name or group password
  - Change the certificate you want to use
- Connections tab
  - Enable, add, and remove backup server connections
  - Connect to the Internet via Dial-Up Networking

See the appropriate section of this chapter for each tab and parameter.

4.511
J

Step 4 When you have finished setting parameters, click **OK**. The Properties dialog box closes and the VPN Dialer saves your changes.

To discard your changes, click **Cancel**. The Properties dialog box closes and discards all changes.

Changing General Settings

The Properties > General tab lets you set general parameters for this connection entry. (See Figure 3-17.)

Changing Connection Entry Description

To change the description of this connection entry, enter or edit the description field. This field is optional, but it can help you identify this connection.

Enabling Transparent Tunneling

Transparent tunneling allows secure transmission between the VPN Client and a secure gateway through a router serving as a firewall, which may also be performing Network Address Translation (NAT) or Port Address Translations (PAT). Transparent tunneling encapsulates Protocol 50 (ESP) traffic within UDP packets and can allow for both IKE (UDP 500) and Protocol 50 to be encapsulated in TCP packets before they are sent through the NAT or PAT devices and/or firewalls. The most common application for transparent tunneling is behind a home router performing PAT.

The VPN Client also sends keepalives frequently, ensuring that the mappings on the devices are kept active.

Not all devices support multiple simultaneous connections behind them. Some cannot map additional sessions to unique source ports. Be sure to check with your device's vendor to verify whether this limitation exists. Some vendors support Protocol-50 (ESP) Port Address Translation (IPSec passthrough), which might let you operate without enabling transparent tunneling.

To use transparent tunneling, the central-site group in the Cisco VPN device must be configured to support it. For an example, refer to the VPN 3000 Concentrator Manager, Configuration | User Management | Groups | IPSec tab (refer to *VPN 3000 Series Concentrator Reference Volume 1: Configuration* or Help in the VPN 3000 Concentrator Manager browser).

This parameter is enabled by default. To disable this parameter, clear the check. We recommend that you always keep this parameter checked.

Then select a mode of transparent tunneling, over UDP or over TCP. The mode you use must match that used by the secure gateway to which you are connecting. Either mode operates properly through a PAT device. Multiple simultaneous connections might work better with TCP, and if you are in an extranet environment, then in general, TCP mode is preferable. UDP does not operate with stateful firewalls so in this case, you should use TCP.

RQS Nº 03/2005 - CN
CPMI 3-17 EIOS
0971
Fls:
3701
Doc:

Allow IPSec over UDP (NAT/PAT)

To enable **Allow IPSec over UDP**, click the radio button. With UDP, the port number is negotiated. UDP is the default mode.

Use IPSec over TCP (NAT/PAT/Firewall)

To enable **Use IPSec over TCP**, click the radio button. When using TCP, you must also enter the port number for TCP in the TCP port field. This port number must match the port number configured on the secure gateway. The default port number is 10000.

Note When using the VPN Client behind an ESP-aware NAT/Firewall, the port on the NAT/Firewall device may be closed due to the VPN Client's keepalive implementation, called DPD (Dead Peer Detection). When a client is idle, it does not send a keepalive until it sends data and gets no response.

To allow the VPN Client to work through ESP-aware NAT/Firewalls, add the ForceKeepAlives parameter to the *.pcf (profile configuration file) for the affected connection profile. This parameter enables IKE and ESP keepalives for the connection at approximately 20 second intervals.

Use the following syntax when adding this parameter to the [Main] section of any *.pcf file:

ForceKeepAlives=1

For more information, see "Connection Profile Configuration Parameters" in the *VPN Client Administrator Guide*.

Allowing Local LAN Access

The Allow Local LAN Access parameter gives you access to the resources on your local LAN (printer, fax, shared files, other systems) when you are connected through a secure gateway to a central-site VPN device. When this parameter is enabled and your central site is configured to permit it, you can access local resources while connected. When this parameter is disabled, all traffic from your Client system goes through the IPSec connection to the secure gateway.

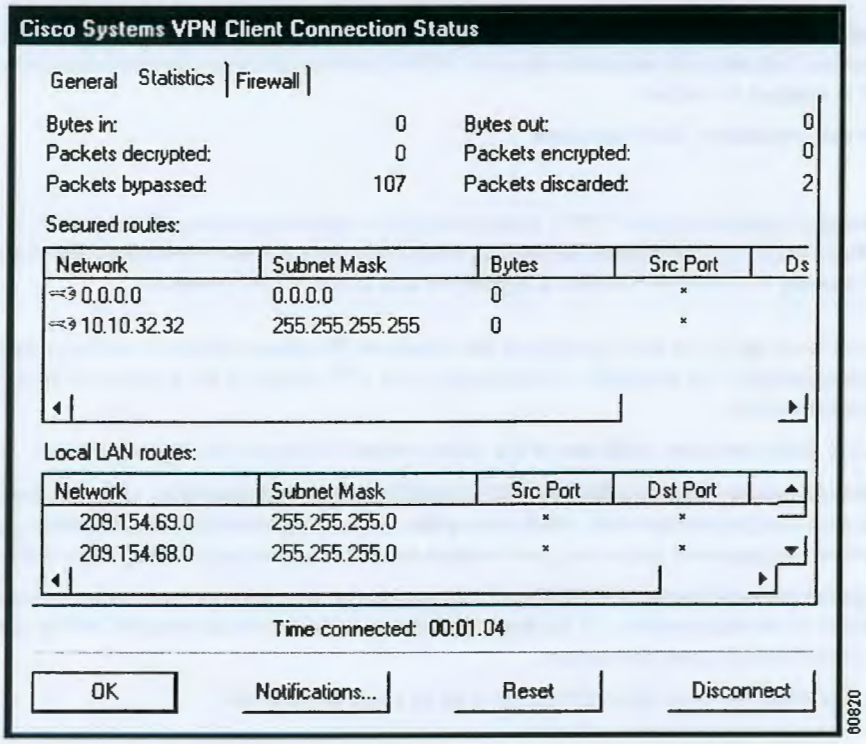
To enable this feature, check **Allow Local LAN Access**; to disable it, clear the check mark from the box. If the local LAN you are using is not secure, you should disable this feature. For example, you would disable this feature when you are using a local LAN in a hotel or airport.

A network administrator at the central site configures a list of networks at the Client side that you can access. You can access up to 10 networks when this feature is enabled. When Allow Local LAN Access is enabled and you are connected to a central site, all traffic from your system goes through the IPSec tunnel except traffic to the networks excluded from doing so (in the network list).

When this feature is enabled and configured on the VPN Client and permitted on the central-site VPN device, you can see a list of the local LANs available by looking on the Statistics tab on the Connection Status dialog box. (See Figure 3-18.)

Note This feature works only on one NIC card, the same NIC card as the tunnel.

Figure 3-18 Local LAN Access



The Local LAN routes section on the Connection Status dialog box lists the IP address and subnet mask of each available network. The Src Port and Dst Port fields are not currently used.

Note While connected, you cannot print or browse the local LAN by name; when disconnected, you can print and browse by name. For more information on this limitation refer to *VPN Client Administrator Guide*, Chapter 1.

Adjusting the Peer Response Timeout Value

The VPN Client uses a keepalive mechanism called Dead Peer Detection (DPD) to check the availability of the VPN device on the other side of an IPSec tunnel. If the network is unusually busy or unreliable, you may need to increase the number of seconds to wait before the VPN Client decides that the peer is no longer active. The default number of seconds to wait before terminating a connection is 90 seconds. The minimum number of seconds you can configure is 30 seconds and the maximum is 480 seconds.

To adjust the setting, enter the number of seconds in the **Peer response timeout** field.

The VPN Client continues to send DPD requests every 5 seconds, until it reaches the number of seconds specified by the Peer response timeout value.

Logging on to Microsoft Network (Windows 95, Windows 98, and Windows ME)

The **Logon to Microsoft Network** parameter registers your PC on the private Microsoft network and lets you browse and use network resources after the VPN Client establishes a secure connection. This parameter is enabled by default.

To disable this parameter, clear the check.

Note This parameter appears only on VPN Clients installed on systems running Windows 95, Windows 98, and Windows ME. For information on logging on to Windows NT and Windows 2000 systems, see the section "Starting a Connection Before Logging on to a Windows NT Platform."

If you do not need or do not have privileges for Microsoft Windows resources on the private network, disable this parameter. For example, if you require only FTP access to the private network, you could disable this parameter.

If you enable this parameter, click one of the radio buttons to choose the logon process:

Use default system logon credentials—Use the Windows logon username and password on your PC to log on to the private network. With this option, you do not need to manually enter your logon username and password each time you connect to the private network. This is the default selection.

Prompt for network logon credentials—The private network prompts you for a username and password to use its resources. If the logon username or password on your PC differs from those on the private network, use this option.

When you are done with the General tab, click **OK** or click another tab.

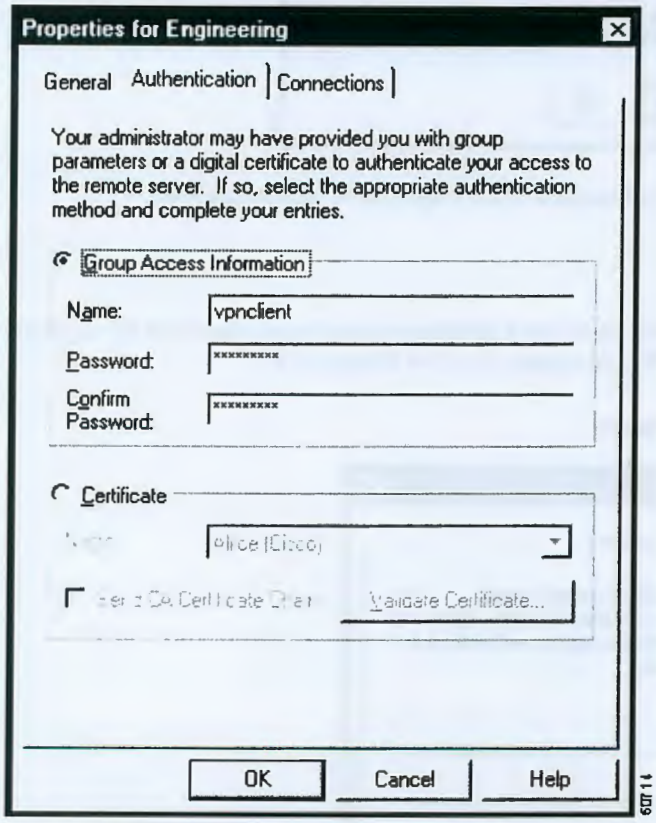
Changing Authentication Settings

The Properties > Authentication tab (see Figure 3-19) lets you change the name or password of the IPSec group to which you are assigned. Your group determines your access to, and use of, the remote network. The group name and password are essential parameters in authenticating you as a user of the remote network.

4.507
1

If you want to choose a different certificate, you also use this screen.

Figure 3-19 Changing Authentication Parameters from the Authentication Tab



Changing Group Name or Group Password

You usually specify a group name and group password when you create a connection entry. However, you can use the Authentication tab to change a group name or group password if your system administrator so instructs you; or to enter the group name and password if the connection entry does not already have them.

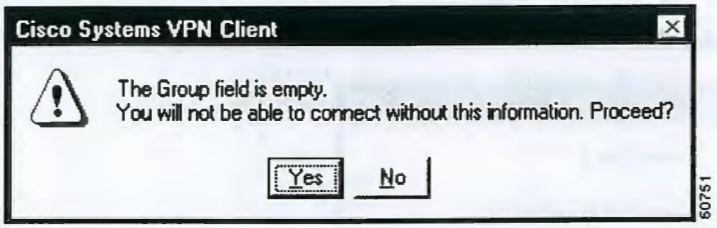
In the Name field, enter or edit the group name. This entry is case-sensitive.

In the Password field, enter or edit the group password. This entry is case-sensitive. The field displays only asterisks. Verify your password by entering it again in the Confirm Password field.

If either field is empty when you leave this dialog box, the VPN Client reminds you to enter missing group information. (See Figure 3-20.) To proceed, click **Yes**, or to terminate, click **No**. If you click No, the message closes, which lets you enter the missing information.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
3-21
0973
Fls:
3701
Doc:

Figure 3-20 Reminder Dialog Box

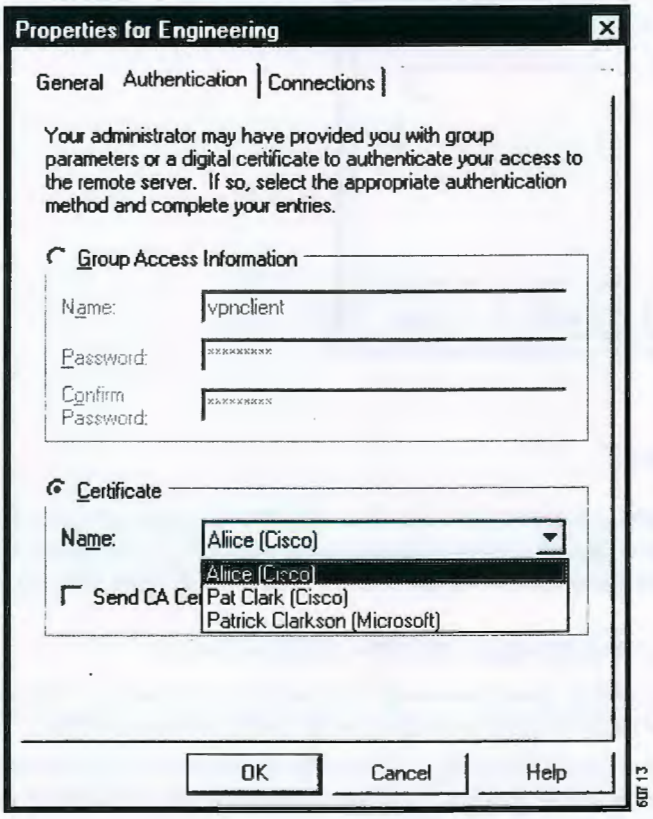


When you are done with the Authentication tab, click **OK** or click another tab.

Choosing a Different Certificate

To choose a different certificate, check the **Certificate** radio button, then click the drop-down menu of certificates installed on your PC and choose one. (See Figure 3-21.)

Figure 3-21 Choosing a Certificate

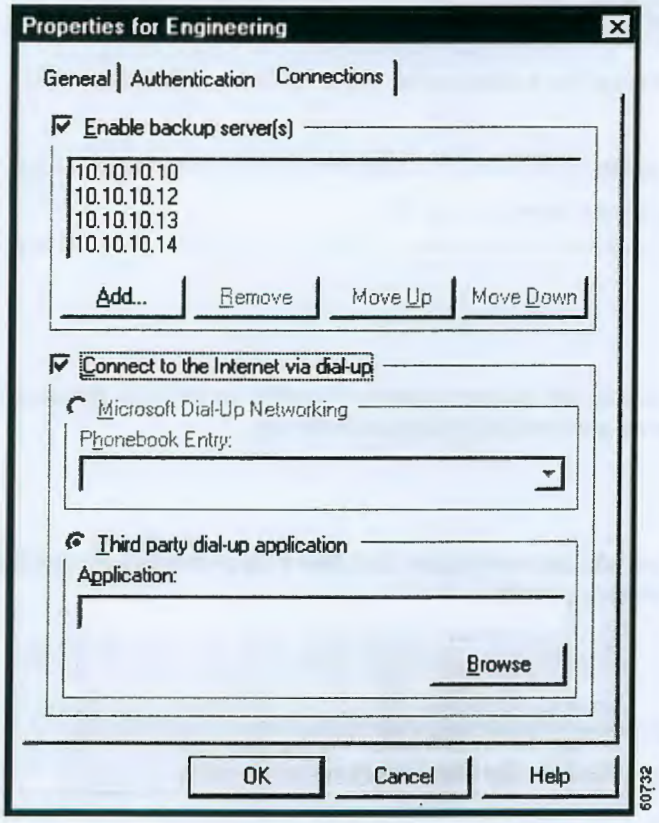


When you are done with the Authentication tab, click **OK** or click another tab.

Changing Connection Settings

The Properties > Connections tab (shown in Figure 3-22) lets you set parameters that govern how you connect to the private network. You can enable and configure backup server connections, and automatically launch a dial-up networking application to connect to the Internet.

Figure 3-22 Changing Parameter Values from the Connections tab



Enabling and Adding Backup Servers

The private network may include one or more backup VPN servers to use if the primary server is not available. Your system administrator tells you whether to enable backup servers. Information on backup servers can download automatically from the VPN Concentrator or you can manually enter this information.

To enable backup servers from the VPN Client, perform the following steps:

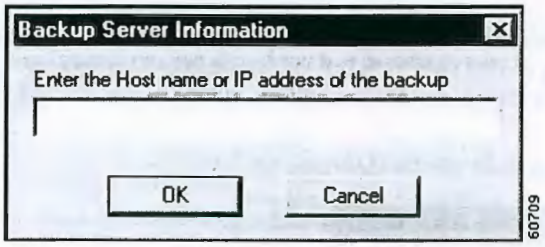
Step 1 Check **Enable backup server(s)**. This is not checked by default.

Step 2 Click **Add** to enter its address.

The Backup Server Information dialog box appears. (See Figure 3-23.)

ROS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 0974
3701
Doc:

Figure 3-23 Entering Backup Server Information



Step 3 Enter the hostname or IP address of the backup server. Use a maximum of 255 characters.

Step 4 Click **OK**.

The hostname or IP address appears in the Enable backup server(s) list. (See Figure 3-22.)

Step 5 To add more backup devices, repeat Steps 2, 3, and 4.

Removing Backup Servers

To remove a server from the backup list, choose the server from the list and click **Remove**. *There is no confirmation or undo.* The server name no longer appears in the list.

Changing the Order of the Servers

To reorder the servers in the list, choose a server and click **Move Up** to increase the server's priority or **Move Down** to decrease the server's priority.

Disabling Backup Servers

You can disable using backup servers without removing backup servers from the list.

To disable using backup servers, clear the **Enable backup server(s)** check.

Configuring a Connection to the Internet Through Dial-up Networking

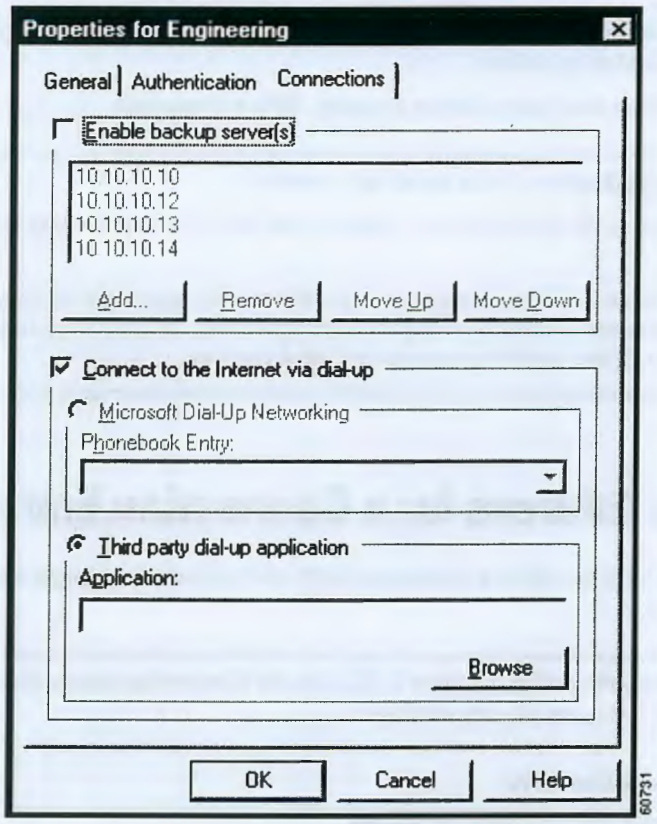
To connect to a private network using a dial-up connection, perform the following two steps:

Step 1 Use a dial-up connection to your Internet service provider (ISP) to connect to the Internet.

Step 2 Use the VPN Client to connect to the private network through the Internet.

To enable and configure this feature, check **Connect to the Internet via dial-up**. This is not checked by default. (See Figure 3-24.)

Figure 3-24 Connecting to the Internet Through Dial-up



You can connect to the Internet using the VPN Dialer application in two different ways:

- Microsoft Dial-up Networking (DUN)
- Third party dial-up program

Microsoft Dial-up Networking

If you have DUN phonebook entries and have enabled Connect to the Internet via dial-up, Microsoft Dial-up Networking is enabled by default. To link a VPN Client connection entry to a Dial-Up Networking phonebook entry, perform the following steps:

Step 1 Click **Microsoft Dial-up Networking** (if it is not already enabled).

Step 2 To link your VPN Client connection entry to a DUN entry, click the down arrow next to the Phonebook entry field and choose an entry from the drop-down menu.

The VPN Client then uses this DUN entry to automatically dial into the Microsoft network before making the VPN connection to the private network.

RQS Nº 03/2005 - CN - CORREIOS
0975
Fls:
3781
Doc:

Third Party Dial-up Program

If you have no DUN phonebook entries and have enabled Connect to the Internet via dial-up, then Third party dial-up application is enabled by default.

To connect to the Internet using a third party dial-up program, follow these steps:

Step 1 Click **Third party dial-up application**, if it is not already enabled.

Step 2 Use **Browse** to enter the name of the program in the **Application** field. This application launches the connection to the Internet.

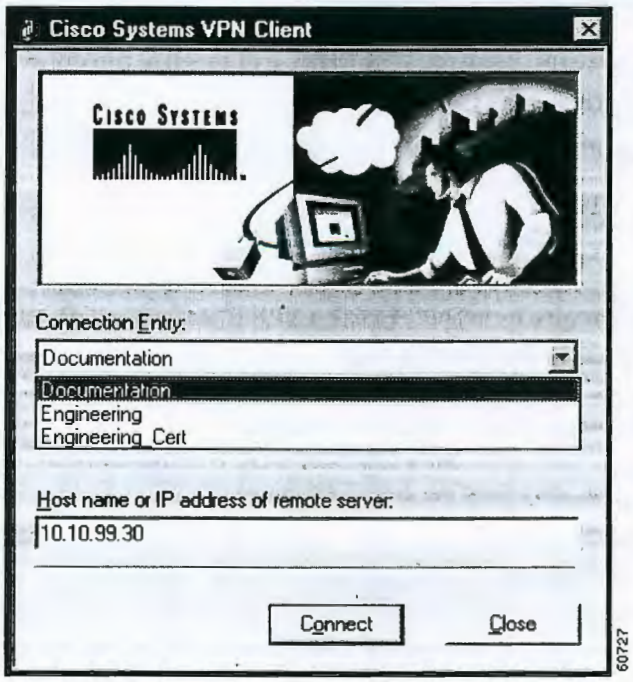
This string you choose or enter here is the pathname to the command that starts the application and the name of the command; for example: c:\isp\ispdialer.exe dialEngineering. Your network administrator might have set this up for you. If not, consult your network administrator.

Changing the VPN Device Address for a Connection Entry

To change the address of the VPN device in a connection entry, and to make the change temporary or permanent, follow these steps:

Step 1 On the VPN Client main dialog box shown in Figure 3-25, click the **Connection Entry** drop-down menu button and choose the entry, if it is not already displayed.

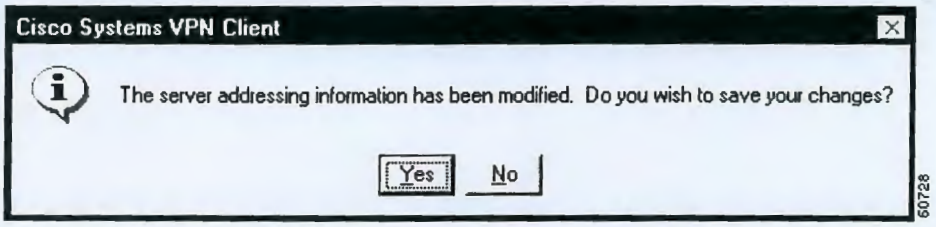
Figure 3-25 Choosing a Connection Entry



Step 2 Edit the address in the Host name or IP address of remote server field.

Step 3 Click **Connect**. The VPN Client displays a confirmation dialog box. (See Figure 3-26.)

Figure 3-26 Confirming Your Changes



Step 4 Click one of the following:

To use this address for the current session only, click **No**. The VPN Client begins connecting to the VPN device, but it does not save the change you have made to the connection entry.

To permanently change the address for this connection entry, click **Yes**. The VPN Client begins connecting to the VPN device, and it saves the new address with the connection entry.

For an explanation of the connection process, see "Connection Procedure".

4.501
3
RQS Nº 03/2005 - CN
CPMI - CORREIOS
0976
Fls:
3701
Doc:

CHAPTER 4

Connecting to a Private Network

This chapter explains how to connect to a private network with the VPN Client.

We assume you have configured at least one VPN Client connection entry as described in "Configuring the VPN Client." To connect to a private network, you also need the following information:

- ISP logon username and password, if necessary.
- User authentication information:
  - If you are authenticated via the VPN 3000 Concentrator internal server, your username and password.
  - If you are authenticated via a RADIUS server, your username and password.
  - If you are authenticated via an Windows NT Domain server, your username, password, and domain name.
  - If you are authenticated via RSA Data Security (formerly SDI) SecurID or SoftID, your username and PIN.
  - If you use a digital certificate for authentication, the name of the certificate and your username and password. If your private key is password protected for security reasons, you also need this password.

Refer to your entries in "Gathering Information You Need," as you complete the steps described here, which include the following sections:

- Starting the VPN Dialer
- Using the VPN Client to Connect to the Internet via Dial-Up Networking
- Authenticating to Connect to the Private Network
- Connecting with Digital Certificates
- Viewing Connection Status
- Closing the VPN Client
- Disconnecting your VPN Client Connection

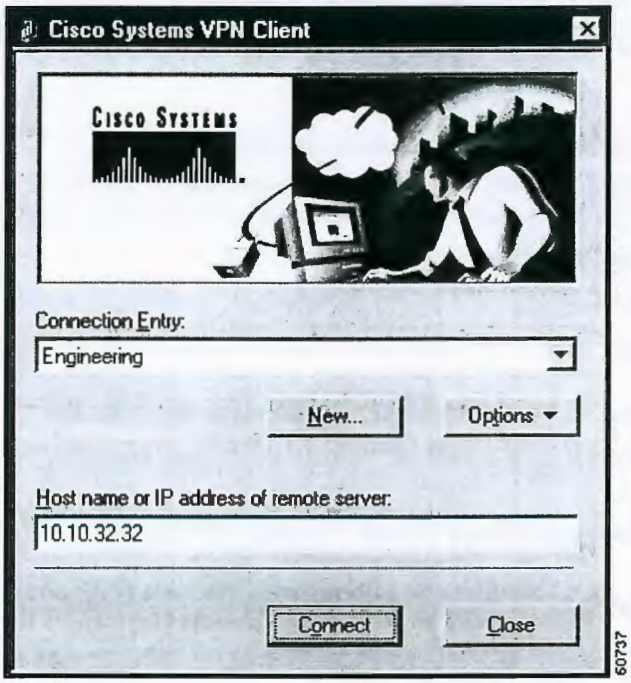
RQS Nº [redacted] - CN
CPMI - CORREIOS
0977
Fls: 3701
Doc:

Starting the VPN Dialer

Step 1 To start the VPN Dialer application, choose **Start > Programs > Cisco Systems VPN Client > VPN Dialer**.

The VPN Dialer displays the VPN Client's main dialog box. (See Figure 4-1.)

Figure 4-1 VPN Dialer Main Dialog Box



Step 2 If necessary, click the **Connection Entry** drop-down menu and choose the desired connection entry.

Connection Procedure

To connect to a private network, perform the following steps:

Step 1 Connect to the Internet, if necessary.

Step 2 Connect to the private network through the Internet.

- Systems with cable or DSL modems are usually connected to the Internet, so no additional action is necessary. Skip to "Authenticating to Connect to the Private Network."
- Systems with modems or ISDN modems must connect to the Internet via Dial-Up Networking:
  - If you connect to the Internet via Dial-up Networking, proceed to "Using the VPN Client to Connect to the Internet via Dial-Up Networking."

- If you must manually connect to the Internet, do it now. When your connection is established, skip to "Authenticating to Connect to the Private Network."
- If your system is already connected to the Internet via Dial-Up Networking, skip to "Authenticating to Connect to the Private Network."

4.498
J

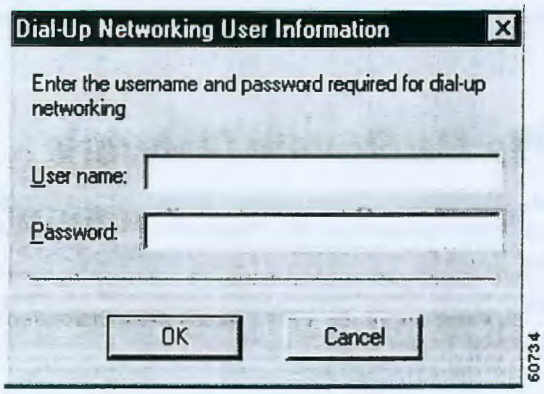
Using the VPN Client to Connect to the Internet via Dial-Up Networking

This section describes how to connect to the Internet via Dial-Up Networking by running only the VPN Client. Your connection entry must be configured with Connect to the Internet via Dial-Up Networking enabled; see "Configuring the VPN Client".

Step 1 Click **Connect** on the VPN Client's main dialog box. (See Figure 4-1.)

If your credentials are not stored in the RAS database, the Dial-up Networking User Information dialog box appears. (See Figure 4-2.) This dialog box varies depending on the version of Windows you are using.

Figure 4-2 Entering User Information



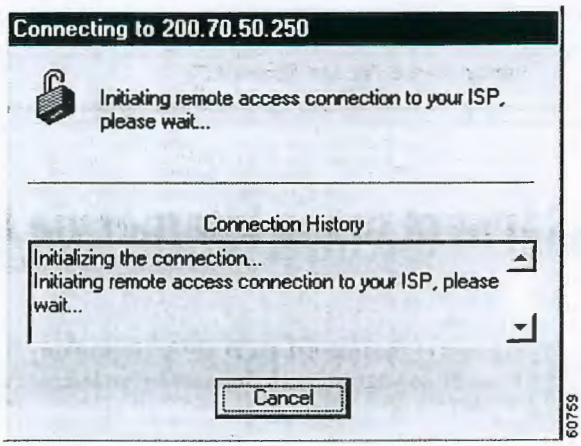
Step 2 Enter your username and password to access your ISP. These entries may be case-sensitive. The Password field displays only asterisks.

Step 3 Click **OK**.

You see the Connection History dialog box. (See Figure 4-3.)

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0978
Fls:
3701
Doc:

Figure 4-3 Confirming Connections to ISP



When the ISP connection is established, a Dial-Up Networking icon appears in the system tray on the Windows task bar. (See Figure 4-4.)

Figure 4-4 Dial-Up Networking task bar Icon

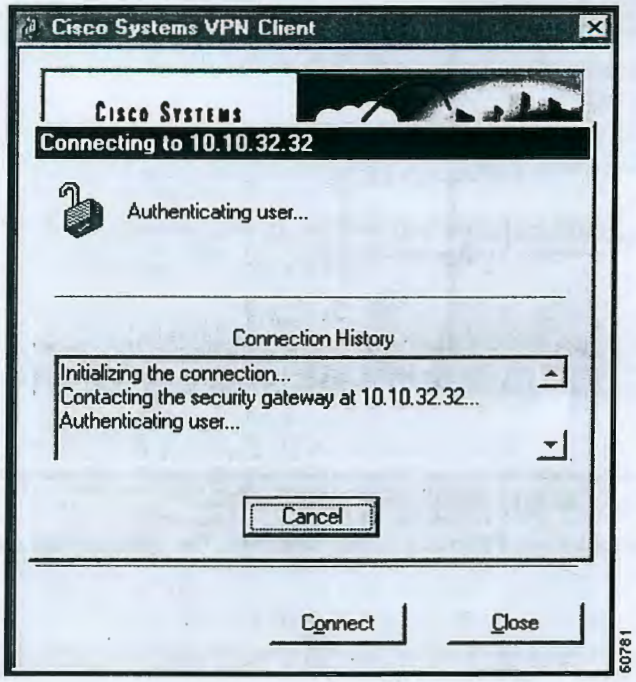
Authenticating to Connect to the Private Network

This section assumes you are connected to the Internet. If you connect using Dial-Up Networking, verify that its icon is visible in the Windows task bar system tray. (See Figure 4-4.) If not, your Dial-Up Networking connection is not active and you need to establish it before continuing.

If you did not do so earlier, click **Connect** on the VPN Client's main dialog box. (See Figure 4-1.)

The VPN Client starts tunnel negotiation and displays the Connection History dialog box. (See Figure 4-5.)

Figure 4-5 Negotiating Dialog Box



The next phase in tunnel negotiation is user authentication.

User Authentication

User authentication means proving that you are a valid user of this private network. User authentication is optional. Your administrator determines whether it is required.

The VPN Client displays a user authentication dialog box that differs according to the authentication that your IPSec group uses. Your system administrator tells you which method to use.

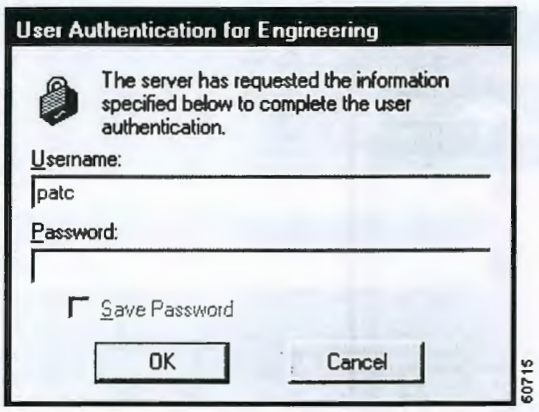
To continue, refer to your entries in "Gathering Information You Need" and go to the appropriate authentication section that follows.

Authenticating Through the VPN Device Internal Server or RADIUS Server

To display the user authentication dialog box, perform the following steps. The title bar identifies the connection entry name.

4.496
RQS Nº 03/2005 - CN - CPMI - CORREIOS
Fls: 0979
Doc: 3701

Figure 4-6 Authenticating Through an Internal or RADIUS Server



Step 1 In the Username field, enter your username. This entry is case-sensitive.

Step 2 In the Password field, enter your password. This entry is case-sensitive. The field displays only asterisks.

Step 3 Click **OK**.

Note If you cannot choose the Save Password option, your administrator does not allow this option. If you can choose this option, be aware that using it might compromise system security, since your password is then stored on your PC and is available to anyone who uses your PC.

If Save Password is checked and authentication fails, your password may be invalid. To eliminate a saved password, click **Options** > **Erase User Password**.

Proceed to the section "Viewing Connection Status."

Authenticating Through a Windows NT Domain

To display the Windows NT Domain user authentication dialog box, perform the following steps. The title bar identifies the connection entry name.

Figure 4-7 Authenticating Through a Windows NT Domain

Step 1 In the Username field, enter your username. This entry is case-sensitive.

Step 2 In the Password field, enter your password. This entry is case-sensitive. The field displays only asterisks.

Step 3 In the Domain field, enter your Windows NT Domain name, if it is not already there.

Step 4 Click **OK**.

Skip to "Viewing Connection Status."

Changing your Password

Your network administrator may have configured your group for RADIUS with Expiry authentication on the VPN 3000 Concentrator. If this feature is in effect and your password has expired, a dialog box prompts you to enter and confirm a new password.

After you have tried unsuccessfully to log in three times, you might receive one of the following login messages:

- Restricted login hours
- Account disabled
- No dial-in permission
- Error changing password
- Authentication failure

These messages let you know the cause of your inability to log in. For help, contact your network administrator.

4.494
RQS Nº 03/2005 - CN - CPMI - CORREIOS
4-7
Fls: 0980
3701
Doc:

Authenticating Through RSA Data Security (RSA) SecurID (SDI)

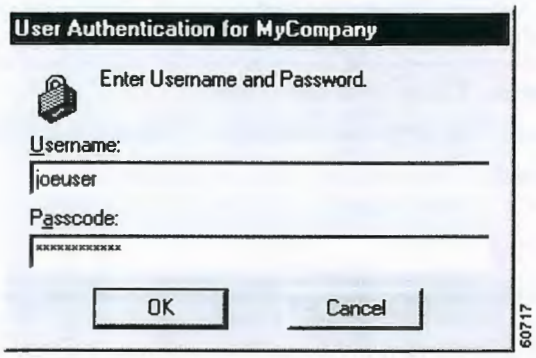
RSA (formerly SDI) SecurID authentication methods include physical SecurID cards and keychain fobs, and PC software called SoftID. SecurID cards also vary: with some cards, the passcode is a combination of a PIN and a cardcode; with others, you enter a PIN on the card and it displays a passcode. Ask your system administrator for the correct procedure.

Authentication via these methods also varies slightly for different operating systems. If you use an RSA method, the VPN Client displays the appropriate RSA user authentication dialog box. The title bar identifies the connection entry name.

RSA User Authentication: SecurID Tokencards (Tokencards, Pinpads, and Keyfobs) and SoftID v1.0 (Windows 95, Windows 98, and Windows ME)

To display an authentication dialog box asking for your username and passcode, perform the following steps. (See Figure 4-8.) If you are using SoftID, it must be running on your PC.

Figure 4-8 Authenticating through RSA



Step 1 In the Username field, enter your username. This entry is case-sensitive.

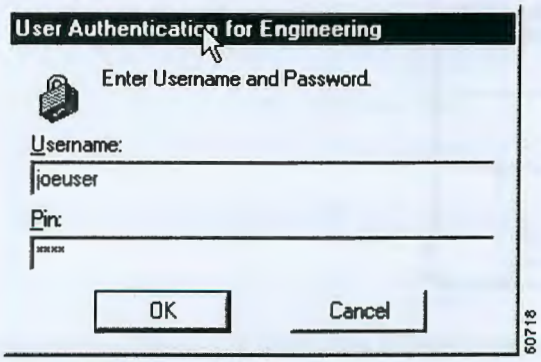
Step 2 In the Passcode field, enter a SecurID code. With SoftID, you can copy this code from the SoftID window and paste it here. Your administrator will tell you what you need to enter here, depending on the type of tokencard you are using.

Step 3 After entering the code, click **OK**.

RSA User Authentication: SoftID v1.x (Windows NT Only) and SoftID v2.0 (All Operating Systems)

If you are using SoftID under Windows NT, the VPN Client displays an authentication dialog box asking for your username and PIN. (See Figure 4-9).

Figure 4-9 Authenticating Through SoftID on Windows NT



Step 1 In the Username field, enter your username. This entry is case-sensitive.

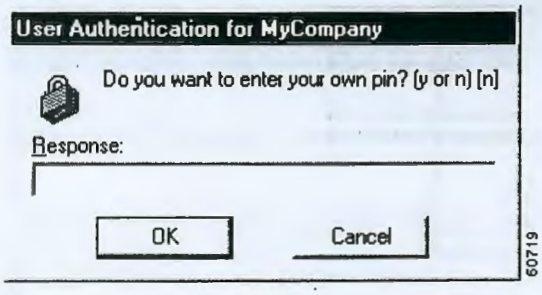
Step 2 In the PIN field, enter your SoftID PIN. The VPN Client gets the passcode from SoftID by communicating directly with SoftID. The SoftID application must be installed but does not have to be running on your PC.

Step 3 After entering the PIN, click **OK**.

RSA New PIN Mode

The first time you authenticate using SecurID or SoftID (all operating systems), or if you are using a new SecurID card, and if the RSA administrator allows you to create your own PIN, the authentication program asks if you want to create your own PIN. (See Figure 4-10.)

Figure 4-10 SecurID New PIN Request

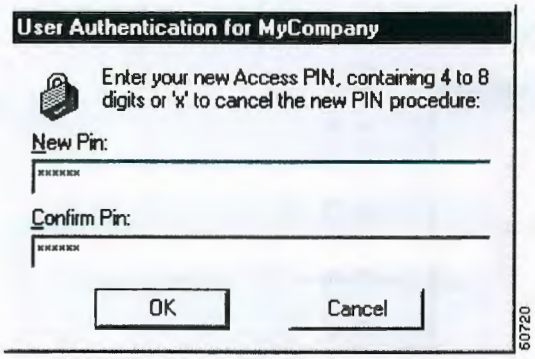


Step 1 Enter your response **y** for yes or **n** for no. No is the default response. Then, click **OK**. What happens next depends on your response.

ROS Nº 03/2005 - CN
CPMI - CORREIOS
0981
Fls:
3701
Doc:

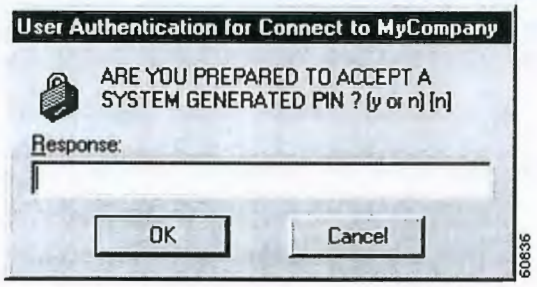
- If you responded yes—Enter your new PIN in the New PIN field and enter it again in the Confirm PIN field. Click **OK**. (See Figure 4-11.)

Figure 4-11 Entering a New PIN Yourself



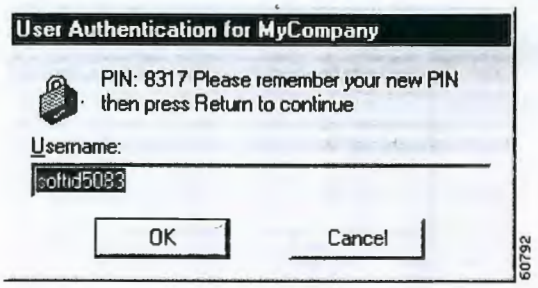
- If you responded no—the authentication program asks if you will accept a system-generated PIN. (See Figure 4-12.)

Figure 4-12 Accepting a PIN from the System



Step 2 To receive a PIN, you must respond **y** for yes and then click **OK**. When you do, the authentication program generates a PIN for you and displays it. (See Figure 4-13.) Be sure to remember your PIN.

Figure 4-13 New PIN Received



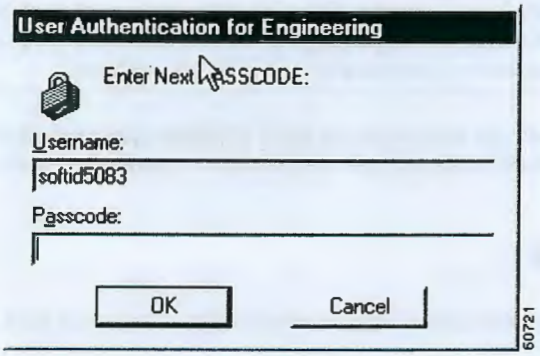
Step 3 To continue, click **OK**.

SecurID Next Cardcode Mode

Sometimes SecurID authentication prompts you to enter the next cardcode from your token card, as in Figure 4-14. SecurID displays this prompt either to resynchronize the token card with the RSA server, or because it noticed several unsuccessful attempts to authenticate with this username.

The SecurID Next Cardcode Mode dialog box might appear. (See Figure 4-14.)

Figure 4-14 Entering the Passcode for SecurID Next Card



In the Passcode field, enter the next code from your token card. This field requires only a cardcode. Do not include your PIN as part of the passcode.

Now continue to "Viewing Connection Status."

Connecting with Digital Certificates

Before you created a connection entry using a digital certificate, you must have already enrolled in a Public Key Infrastructure (PKI), have received approval from the Certificate Authority (CA), and have one or more certificates installed on your system. If this is not the case, then you need to obtain a digital certificate. In many cases, the network administrator of your organization can provide you with a certificate. If not, then you can obtain one by enrolling with a PKI directly using the Certificate Manager application, or you can obtain an Entrust profile through Entrust Entelligence. Currently, we support the following PKIs:

- UniCERT from Baltimore Technologies (www.baltimoretechnologies.com)
- Entrust PKI™ from Entrust Technologies (www.entrust.com)
- Versign (www.verisign.com)
- Microsoft Certificate Services in Microsoft Windows 2000 Server
- Cisco Certificate Store

The websites listed in parentheses in this list contain information about the digital certificates that each PKI provides. The easiest way to enroll in a PKI or import a certificate is to use the Certificate Manager (see "Enrolling and Managing Certificates") or Entrust Entelligence (see Entrust documentation).

RQS Nº 03/2005 - CN - CPMI - CORREIOS
Fls: 0982
Doc: 3701

Note Every time you connect using a certificate, the VPN Client checks to verify that your certificate has not expired. If your certificate is within one month of expiring, the VPN Client displays a message when you attempt to connect or when you use the Properties option. The message displays the certificate common name, the "not before" date, the "not after" date, and the number of days until the certificate expires or since it has expired.

There is one exception to this rule. When you are authenticating with a Microsoft certificate, the VPN Dialer skips the automatic certificate validation process and starts the connection immediately. If there is a problem with the certificate, the connection attempt fails. To obtain information about the failure, look in the connection log file (see "Viewing and Managing the VPN Client Event Log"). To validate the certificate manually, choose Properties > Authentication > Validate Certificate.

What happens when you press **Connect** can depend on the level of private key protection on your certificate. If your certificate is password protected, you are prompted to enter the password.

Connecting with an Entrust Certificate

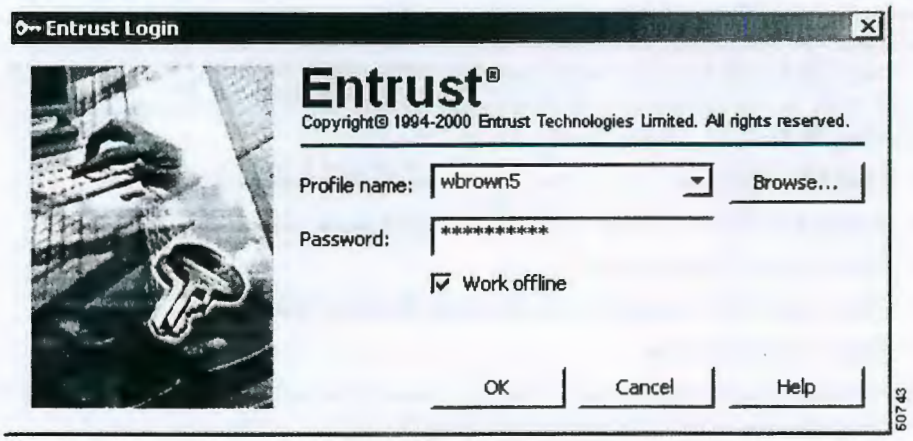
This section provides important information about what to expect when connecting with an Entrust certificate under certain conditions.

Accessing Your Profile

If you are not already logged in, you must log in to Entrust Entelligence to access your Entrust Entelligence certificate profile, using the following procedure:

After you choose **Connect** on the VPN Client main dialog box, the Entrust logon dialog box appears. (See Figure 4-15.)

Figure 4-15 Logging in to Entrust



4.488

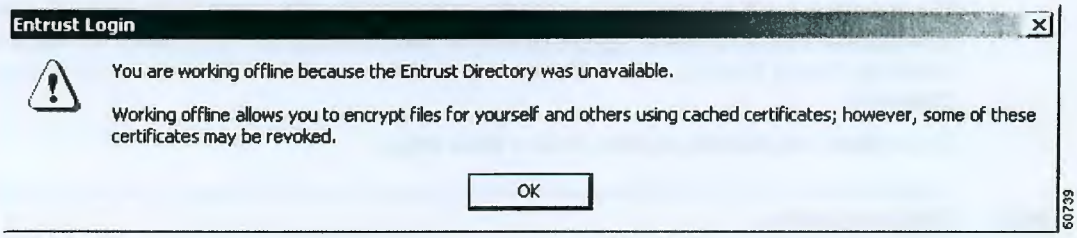
Step 1 Choose a profile name from the pull-down menu.

Your network administrator has previously configured one or more profiles for you through Entrust Entelligence. If the software is installed on your system but there are no profiles available, then you need to get a profile from your network administrator or directly through Entrust. Refer to *Entrust Entelligence Quick Start Guide* for instructions on obtaining a profile. The *VPN Client Administrator Guide* contains supplementary configuration information.

Step 2 After choosing a profile, enter your Entrust password.

Check the Work offline field to use Entrust Entelligence without connecting to the Entrust PKI. If Work offline is checked and you press **OK**, the Entrust wizard displays the message shown in Figure 4-16.

Figure 4-16 Entrust Login Message

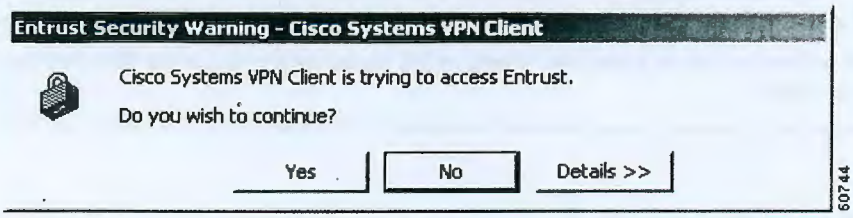


You can ignore this message. Since you are connecting to your organization's private network using an existing certificate profile, you are not interacting with the Entrust PKI. If you see this message, click **OK** to continue.

Step 3 After completing the Entrust Login dialog box (see Figure 4-15), click **OK**.

You may receive a security warning message from Entrust. This warning occurs, for example, when an application attempts to access your Entelligence profile for the first time or when you are logging in after a VPN Client software update. The message happens because Entrust wants to verify that it is acceptable for the VPN Client to access your Entrust profile.

Figure 4-17 Entrust Security Warning



Step 4 At the warning message, click **Yes** to continue.

You can now use your Entrust certificate for authenticating your new connection entry.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 0983
Doc: 5701

Entrust Inactivity Timeout

If you have a secure connection and you see a padlock next to the Entelligence icon in the Windows system tray, Entelligence has timed out. However, you have not lost your connection. If you see the Entelligence icon with an X next to it, you are logged out of Entrust, and you did not have a secure connection initially. To make a new connection, start from the beginning (see "Accessing Your Profile").

Using Entrust SignOn and Start Before Logon Together

Entrust SignOn™ is an optional Entrust application that lets you use one login and password to access Microsoft Windows and Entrust applications. This application is similar to *start before logon*, which is a VPN Client feature that enables you to dial in before logging on to Windows NT. For information about start before logon, see "Starting a Connection Before Logging on to a Windows NT Platform".

If you want to use these two features together, you should make sure you have installed Entrust Entelligence with the Entrust SignOn module before installing the VPN Client. For information about installing Entrust SignOn, refer to Entrust documentation and the *VPN Client Administrator Guide*, Chapter 1.

To use these two features together, follow these steps:

Step 1 Start your system.

When the SignOn option is installed, Entrust displays its own Ctrl Alt Delete dialog box.

Step 2 Click **Ctrl Alt Delete**.

The Entrust Options dialog box and the VPN Dialer login dialog box both pop up. The VPN Dialer dialog box is active.

Step 3 To start your VPN connection, click **Connect** on the VPN Dialer main dialog box.

The Entrust login dialog box becomes active.

Step 4 To log in to your Entrust profile, enter your Entrust password.

The VPN Dialer password prompt dialog box becomes active.

Step 5 Enter your VPN dialer username and password.

The VPN Client authenticates your credentials and optionally displays a banner and/or a notification. Respond to the banner or notification as required. Then the Windows NT logon dialog box is active.

Step 6 To complete the connection, enter your Windows NT logon credentials in the Windows logon dialog box and you are done.

Connecting with a Smart Card or Token

The VPN Client supports authentication with digital certificates through a smart card or electronic token. Several vendors provide smart cards and tokens. For an up-to-date list of those that the VPN Client currently supports, see "Smart Cards Supported". Smart card support is provided through Microsoft Cryptographic API (MS CAPI). Any CryptoService provider you use must support signing with CRYPT_NOHASHOID.

tunnel
definition 1-2
negotiation 4-4
transparent 3-17

U

UDP protocol
firewalls 4-30
transparent tunneling 3-17
UniCERT 4-11
installing the VPN Client
InstallShield 5-29
MSI 5-32
upgrade notification 5-25
upgrading VPN Client software
using InstallShield 5-27
using MSI 5-29
URL or Network Address of CA 6-7
user authentication 1-4, 4-5
see also authentication
username
internal server authentication 4-6
ISP logon 4-3
NT Domain authentication 4-7
RADIUS authentication 4-6
RSA authentication 4-8, 4-9

V

verifying a certificate 3-10, 6-20
version
VPN Client
displaying 3-3
viewing
certificate 6-18
connection status 4-24
enrollment request 6-26
Virtual Private Network (VPN)
defined 1-1
VPN
defined 1-1
VPN Client
applications 1-1
event log 5-17
features 1-3
installing 2-1
software updates 5-27, 5-29
version 3-3
VPN Client version 3.6
removing 2-8
VPN Concentrator
see VPN device
VPN device
authentication using internal server 4-5
backup 3-23
changing address 3-26
Cisco 1-1
DPD 3-19
hostname 3-7
IP address 3-7
notifications 5-25
VPN Dialer
closing 4-32
main dialog box 3-6

W

Windows
NT logon properties 5-14
platforms requirement 2-1
username and password 3-20
wizard
connection entry 3-6
WLANs
auto initiation 4-16

E C T
4.3921
C L A C
RQS Nº 03/2005 - CN
CPMI - CORREIOS
0984
IN-11
Fls:
3701
Doc:

X

X.509 DER file **6-12**

Z

Zone Labs Integrity **4-25, 4-27, 4-31**

INDEX

Numerics

802.11x networks
  wireless LANs **4-16**

A

accessing local LAN **3-18**
adapter card for network **2-2**
adding
  backup servers **3-23**
  connection entry **3-5**
address
  remote server
    changing **3-26**
  VPN device **3-7**
Administrator privileges **2-1**
AES algorithm **1-5**
algorithms
  AES **1-5**
  authentication **1-5**
  DES **1-5**
  encryption **1-5**
  HMAC **1-5**
  MD5 **1-5**
  SHA-1 **1-5**
  triple-DES **1-5**
Application Launcher **5-11**
Are You There see AYT firewall policy
authentication
  algorithms **1-5**
  certificate **2-2, 3-8**
  Entrust **3-10**
  features in VPN Client **1-4**
  information
    connection status **4-25**
  internal server **1-4, 4-5**
  methods **1-4, 4-5**
  NT Domain **1-4**
    dialog box **4-6**
    domain name **4-7**
    password **4-7**
    username **4-7**
  properties
    changing **3-20**
  RADIUS **4-5**
  RSA
    next cardcode **4-11**
    passcode **4-8**
    PIN **4-9**
    username **4-8, 4-9**
  SDI
    seeRSA
  SecurID **1-4, 4-8**
  smart card **4-14**
  SoftID **1-4, 4-8**
auto initiation
  authenticating **4-18**
  changing option values **4-20**
  connection failures **4-22**
  connection profile **4-17**
  disabling **4-20, 5-17**
  disabling while suspended **4-21**
  disconnecting **4-19**
  enabling **4-21, 5-17**
  managing **5-16**

ECT
1H.402
CPL - AC
RQS Nº 03/2005 - CN
CPMI - CORREIOS
0985
Fls:
3701
Doc:

restarting 4-21
resuming 4-19
retry interval 5-17
states 4-23
suspending 4-19
system tray icons 4-23
using 4-16
Automatic VPN Initiation option 5-16
AYT firewall policy 4-25, 4-28

B

b[illegible]p servers
adding 3-23
disabling 3-24
enabling 3-23
removing 3-24
Baltimore Technologies 4-11
base 64 encoded file type 6-12
binary encoded file type 6-12
bytes in
connection statistics 4-26
bytes out
connection statistics 4-26

C

ca[illegible]
connection 1-2
modem 1-2, 4-2
CA certificates 6-5
Centralized Protection Policy see CPP firewall policy
certificate
changing 3-22
changing password 6-22
completing enrollment form 6-4
connecting 4-11
deleting 6-21
enrollment
file types 6-12
PKI 4-11
with CA 6-4
Entrust 3-10
expiring 4-12
exporting 6-23
importing 6-15
managing 6-17
name 3-5, 3-8, 4-1
stores 6-3
verifying 3-10, 6-20
viewing 6-18
Certificate Authorities (CA)
CA certificates tab 6-5
certificate 2-2
supported 4-11
Certificate Manager
Options menu 6-17
overview 6-1
starting 6-2
changing
certificate 3-22
certificate password 6-22
connection entry description 3-17
connection entry properties 3-14
group name or group password 3-21
password on an enrollment request 6-28
remote server address 3-26
Cisco certificate store 6-3
classes that generate events 5-22
clearing events display 5-24
Client/Server policy
firewalls 4-25, 4-27, 4-31
Client IP address in connection status 4-24
cloning a connection entry 5-3
closing the VPN Client 4-32
common name in certificate enrollment 6-4
company in certificate enrollment 6-4

completing an enrollment request 6-29
compression algorithm
LZS compression 4-25
configuring connections automatically 5-5
connecting
before logon 5-14
to private network 4-2, 4-4
to the internet
via Dial-Up Networking 3-24
to the internet via Dial-Up Networking 4-3
with certificate 4-1
nection
LAN 1-2
network
direct 2-2
properties
changing 3-23
statistics
bytes in 4-26
bytes out 4-26
packets bypassed 4-26
packets decrypted 4-26
packets discarded 4-26
packets encrypted 4-26
resetting 4-32
status
key icon 4-27
local LAN routes list 4-27
secure associations 4-27
secured routes 4-27
time connected 4-27
transparent tunneling 4-25
viewing 4-24
technologies 1-2
connection entry
changing
remote server address 3-26
changing description 3-17
changing properties 3-14
cloning 5-3
creating 3-5
creating shortcut 5-10
definition 3-1
deleting 5-4
description 3-17
managing 5-2
optional parameters 3-14
parameters 3-1
preconfigured 3-1
profile 3-5
properties
changing 3-14
renaming 5-5
copyrights and licenses A-1
country code in certificate enrollment 6-5
CPP firewall policy 4-25, 4-29
creating
connection entry 3-5
shortcut for connection entry 5-10

D

data
formats xii
Data Encryption Standard
see DES algorithm
Dead Peer Detection
see DPD
deleting
certificate 6-21
connection entry 5-4
enrollment request 6-27
department in certificate enrollment 6-4
DES algorithm 1-5
DHCP request 1-3
DHCP traffic
stateful firewall always on 5-11

ECT 1.4.400 1 J CPL - AC

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 0500
Doc: 3701

Dial-Up Networking
closing before uninstall 5-29
connecting 3-24, 4-3
dial-up modem 1-2
disabling 3-25
enabling 3-25
icon on taskbar 4-4
Microsoft 1-3
phonebook entries 3-25
programs
third party 3-26
requirement for 2-2
r Information dialog box 4-3
Digital Subscriber Line
see DSL
direct network connection 2-2
disabling
application launch before startup 5-15
automatic disconnect when logging off Windows NT 5-16
backup servers 3-24
Dial-Up Networking 3-25
local LAN access 3-18
Logon to Microsoft Network parameter 3-20
third party dial-up 3-26
disconnecting
automatic 5-16
ate network 4-32
Disk icon in log viewer 5-24
displaying
help 3-1
software version 3-3
DNS
dynamic 1-3
split 1-4
documentation
cautions xii
notes xii
domain
Certificate Authority 6-7
name
certificate enrollment 6-5
NT Domain authentication 4-7
server 1-4
DPD
adjusting peer time out 3-19
keep alive mechanism
DSL
connection technology 1-2
modem 1-2, 4-2
DUN phonebook entries 3-26

E

e-mail address in certificate enrollment 6-5
enabling
auto initiation 5-17
backup servers 3-23
local LAN access 3-18
logging on to Microsoft Network 3-20
start before logon 5-14
stateful firewall 5-11
transparent tunneling 3-17
encryption
algorithms 1-5
connection status 4-25
enrolling
certificates 6-4
file request 6-11
network 6-6
in a PKI 4-11
enrollment request
changing password 6-28
completing 6-29
deleting 6-27
form 6-4
managing 6-25

pasting 6-11
resuming 6-29
viewing 6-26
Entrust
certificate
configuring 3-10
connecting with 4-12
SignOn
using with start before logon 4-14
Technologies 4-11
Erase icon in log viewer 5-24
Erase User Password option 4-6, 5-7
ESP
protocol
transparent tunneling 3-17
traffic
stateful firewall always on 5-11
etoken
connecting with 4-14
events
classes 5-22
collecting 5-19
severity levels 5-21
viewing and managing 5-17
exiting the VPN Client 4-32
exporting a certificate 6-23

F

F1 key
displaying help 3-1
features of VPN Client 1-3
file types for certificate enrollment 6-12
Filter icon in log viewer 5-20
filtering
events 5-20
firewalls 4-29
firewalls 4-30
AYT tab 4-28
Client/Server policy 4-25, 4-27, 4-31
CPP firewall policy 4-29
filtering 4-29
ICMP protocol 4-30
matching 5-26
name on general status
notifications 5-26
policies 4-25
policy listed 4-25
rules 4-29
stateful 5-11
status 4-27
status screen 4-25
support in VPN Client 1-5
tab on status screen 4-25
TCP protocol 4-30
UDP protocol 4-30
force keepalives
ESP-aware NAT 3-18
formats
data xii

G

General tab (Properties) 3-17
generating events
classes 5-22
group name for IPSec
changing 3-21
group password for IPSec
changing 3-21

H

hard disk space requirement 2-2
Hashed Message Authentication Coding
see HMAC algorithm

ECT 1.398 J CPL - AC

RQS Nº 03/2005 - CPMI - CORREIOS
IN-5
Fls: 0987
3701
Doc:

help
displaying 3-1
F1 key 3-1
from program menu 3-1
Help icon in log viewer 5-19
HMAC algorithm 1-5
hostname
VPN device 3-7

I

IANA protocol numbers 4-30
ICMP protocol
firewalls 4-30
icons
Dial-Up Networking 4-4
key 4-27
log viewer
Disk 5-24
Erase 5-24
Filter 5-20
Help 5-19
Printer 5-23
Search 5-22
VPN Client
viewing connection status 4-24
viewing when connected 4-16
VPN Dialer
using to disconnect 4-32
IKE Keepalives 1-4
IKE protocol 1-2
importing
certificate file 6-15
configuration 5-5
Import Password 6-16
inactivity timeout (Entrust) 4-12
installing
media requirements 2-2
installing VPN Client
InstallShield 2-3
MSI 2-5
process 2-1
interface card for network 2-2
internal server
authentication 1-4, 4-5, 4-6
internet
connecting via Dial-Up Networking 3-24, 4-3
Internet Key Management protocol
see IKE
Internet Protocol Security
see IPSec
IOS
platform devices supported x
IP address
certificate enrollment 6-5
server 4-24
VPN device 3-7
IPSec
attributes supported in VPN Client 1-5
features in VPN Client 1-4
group name 3-21
group password 3-21
over TCP 3-18
over UDP 3-18
protocol 1-2
transparent tunneling
connection status 4-25
ISDN
connection technology 1-2
modem 4-2
ISP
password 4-3
username 4-3

E C T
1 4.396 1
J
CPL - AC

K

key icon
  connection status **4-27**

L

LAN connection **1-2**
launching an application **5-11, 5-15**
licenses and copyrights **A-1**
local LAN access **3-18**
  connection status **4-27**
log file
  printing **5-23**
  saving **5-24**
logging on to Microsoft Network **3-20**
log viewer
  clearing **5-24**
  filtering events **5-20**
  icons
    Disk **5-24**
    Erase **5-24**
    Filter **5-20**
    Help **5-19**
    Printer **5-23**
    Search **5-22**
  options
    capture **5-19**
    filter **5-20**
  searching **5-22**
LZS compression **4-25**

M

maintenance dialog
  MSI **2-8**
managing
  auto initiation **5-16**
  certificates **6-1, 6-17**
  connection entries **5-2**
  enrollment request **6-25**
  event log **5-17**
matching firewall configurations **5-26**
Message Digest 5 (MD5) algorithm **1-5**
Microsoft
  Certificate Services **4-11**
  certificate store **6-3**
  Network
    logging on **3-20**
  Windows 2000 **4-11**
  Windows Installer (MSI)
    installing VPN Client **2-5**
modems
  cable **1-2, 4-2**
  dial-up **1-2**
  DSL **1-2, 4-2**
  ISDN **4-2**
  requirement **2-2**
MSI **2-5**
  installation **2-5**
    removing **5-32**
  maintenance dialog **2-8**
  repair dialog **2-8**

N

names
  IPSec group **3-21**
NAT **3-17**
network
  adapter or interface card **2-2**
  connection
    direct **2-2**
Network Address Translation **3-17**
New Connection Entry Wizard **3-6**
notifications
  firewall **5-26**
  upgrade **5-25**

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0988
Fls: IN-7
Doc:
3701

VPN device 5-25
NT Domain authentication 1-4, 4-6
domain name 4-7
password 4-7
username 4-7
NT features
logon 5-14
VPN Client 1-3

O

options
Application Launcher 5-11
auto disconnect 5-16
Automatic VPN Initiation 5-16
Clone entry 5-3
Delete entry 5-4
Erase User Password 5-7
Import entry 5-5
Rename entry 5-5
Save Password 5-7
shortcut 5-10
start before logon 5-14
Stateful Firewall (Always on) 5-11
Windows
Logon Properties 5-14
Options menu 3-14
organizational unit in certificate enrollment 6-4
organization of this manual ix

P

packets
bypassed 4-26
decrypted 4-26
discarded 4-26
encrypted 4-26
parameters
connection entry 3-1
passcode
RSA authentication 4-8
passwords
enrollment request
changing 6-28
erasing 4-6, 5-7
expiration 4-7
import 6-16
internal server authentication 4-6
invalid 4-6
IPSec group
changing 3-21
ISP logon 4-3
NT Domain authentication 4-7
personal certificate 6-22
private key 4-1
RADIUS authentication 4-6
saving 4-6, 5-7
PAT 3-17
Peer Certificate Domain Name Verification 1-4
peer response timeout
adjusting 3-19
personal firewall see firewalls
phonebook entries
DUN 3-26
PIN
RSA authentication 4-9
PKCS10 format 6-12
PKIs
supported 2-2, 4-11
Plain Old Telephone Service
see POTS
port
transparent tunneling 4-25
Port Address Translation 3-17
POTS
connection technology 1-2

preconfigured connection entry 3-1
Printer icon in log viewer 5-23
printing a log file 5-23
private key password 4-1
private network
  connecting 4-2, 4-4
  disconnecting 4-32
privileges required for
  installing VPN Client 2-1
profile
  connection entry 3-5
  Entrust 3-11
  file
    importing into VPN Client 5-5
  roaming 5-16
properties
  general 3-17
Properties dialog box 3-15
Protocol 50 (ESP) traffic 3-17
protocol numbers 4-30
protocols
  DPD
  ESP 3-17
  ICMP 4-30
  IKE 1-2
  IPSec 1-2, 3-18
  TCP 3-17, 4-30
  UDP 3-17, 4-30
Public Key Infrastructure
  see PKIs

Q

quitting the VPN Client 4-32

R

RADIUS authentication
  password 4-6
  procedure 4-5
  username 4-6
RAM requirements 2-2
reconfiguring automatically 5-5
remote access connection
  closing before uninstall 5-29
Remote Authentication Dial-In User Service
  see RADIUS authentication
remote server
  changing address 3-26
removing
  backup servers 3-24
  the VPN Client
    InstallShield 5-29
removing a client configuration
  the VPN Client
    MSI 5-32
renaming a connection entry 5-5
repair dialog
  MSI 2-8
requirements
  system 2-1
resetting connection statistics 4-32
restarting your computer after installation 2-4
resuming an enrollment request 6-29
retry interval
  auto initiation 5-17
roaming profiles 5-16
RSA (formerly SDI)
  authentication 1-4, 4-8
  Next Cardcode 4-11
  passcode 4-8
  PIN 4-9
rules
  firewalls 4-29

ECT 14.3941 CPL - A
RQS Nº 03/2005 - CN
CPMI - CORREIOS
0989
Fls: IN-9
Doc: 3701

S

Save Password option **4-6, 5-7**
saving a log file **5-24**
SCEP (Cisco store) **6-3**
SDI
  see RSA
Search icon in log viewer **5-22**
searching log file **5-22**
secure associations **4-27**
secured routes
  connection status **4-27**
  icon **4-27**
secure gateway
  address **3-7**
  notifications to client **5-25**
Secure Hash Algorithm
  see SHA-1 algorithm
SecurID authentication **1-4, 4-8**
Server IP address
  connection status **4-24**
setting or changing connection entry properties **3-14**
Severity levels in events **5-21**
SHA-1 algorithm **1-5**
shortcut
  creating for connection entry **5-10**
Simple Certificate Enrollment Protocol
  SCEP
smart card
  connecting with **4-14**
  connection entry
    configuring **3-11**
  products supported **3-12**
SoftID authentication **1-4, 4-8**
software license agreement **A-1**
software token applications
  launching from VPN Dialer **5-11**
split DNS **1-4**
split tunneling **1-4**
start before logon
  configuring **5-14**
  using with Entrust SignOn **4-14**
starting the VPN Dialer
  connecting to private network **3-5, 4-2**
  using a shortcut **5-10**
stateful firewall
  always on **5-11**
  DHCP traffic **5-11**
  transparent tunneling **3-17**
state in certificate enrollment **6-4**
statistics
  connection time **4-27**
  local LAN routes **4-27**
  packet **4-26**
  secured routes **4-27**
status
  firewall **4-27**
stopping the VPN Dialer **4-32**
stores
  certificate **6-3**
system requirements **2-1**

T

TCP/IP requirement **2-2**
TCP protocol
  firewalls **4-30**
  transparent tunneling **3-17**
third party dail-up program **3-26**
time connected
  connection status **4-27**
transparent tunneling
  enabling **3-17**
  port **4-25**
  stateful firewall **3-17**
triple-DES algorithm **1-5**

tunnel
definition 1-2
negotiation 4-4
transparent 3-17

U

UDP protocol
firewalls 4-30
transparent tunneling 3-17
UniCERT 4-11
installing the VPN Client
InstallShield 5-29
MSI 5-32
upgrade notification 5-25
upgrading VPN Client software
using InstallShield 5-27
using MSI 5-29
URL or Network Address of CA 6-7
user authentication 1-4, 4-5
see also authentication
username
internal server authentication 4-6
ISP logon 4-3
NT Domain authentication 4-7
RADIUS authentication 4-6
RSA authentication 4-8, 4-9

V

verifying a certificate 3-10, 6-20
version
VPN Client
displaying 3-3
viewing
certificate 6-18
connection status 4-24
enrollment request 6-26
Virtual Private Network (VPN)
defined 1-1
VPN
defined 1-1
VPN Client
applications 1-1
event log 5-17
features 1-3
installing 2-1
software updates 5-27, 5-29
version 3-3
VPN Client version 3.6
removing 2-8
VPN Concentrator
see VPN device
VPN device
authentication using internal server 4-5
backup 3-23
changing address 3-26
Cisco 1-1
DPD 3-19
hostname 3-7
IP address 3-7
notifications 5-25
VPN Dialer
closing 4-32
main dialog box 3-6

W

Windows
NT logon properties 5-14
platforms requirement 2-1
username and password 3-20
wizard
connection entry 3-6
WLANs
auto initiation 4-16

4.3921
RQS Nº 03/2005 - CN
CPMI - CORREIOS
0000
IN-11
Fls:
3701
Doc:

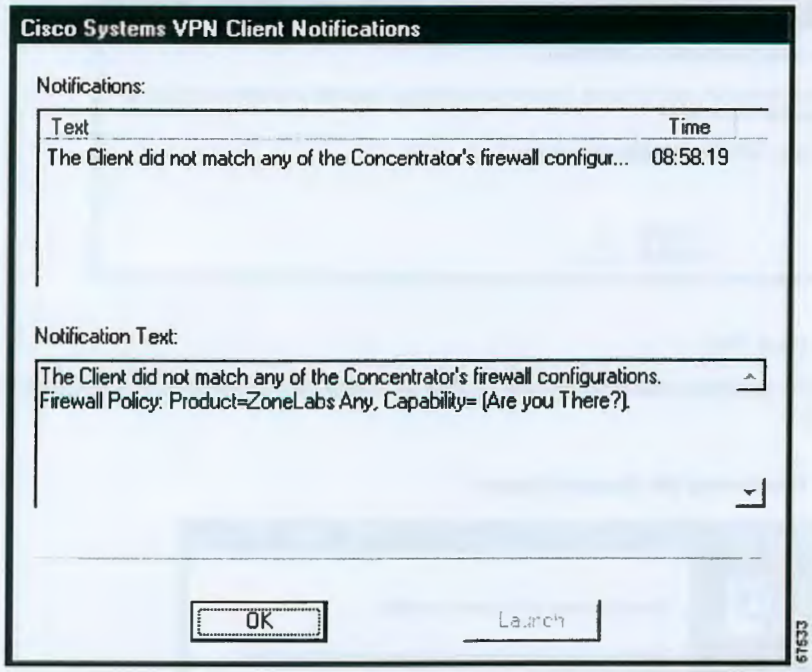
X

X.509 DER file **6-12**

Z

Zone Labs Integrity **4-25, 4-27, 4-31**

Figure 5-28 Firewall Notification



Upgrading the VPN Client Software (InstallShield)

Upgrading the VPN Client software using this method retains existing connection entries and their parameters.

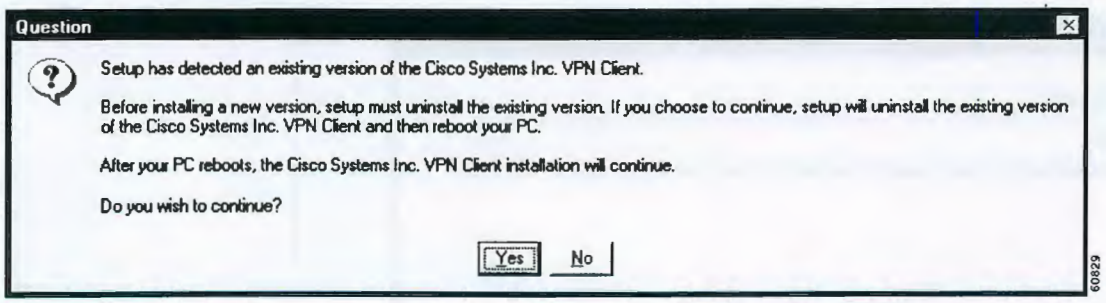
To install an upgrade of the VPN Client over an existing version on your system, use the following procedure, which first uninstalls the existing version, and then reboots your PC and installs the new version.

Step 1 To begin the procedure, follow the instructions in the "Installing the VPN Client Through InstallShield" section in Chapter 2.

When it starts, the installation wizard detects the existing version and asks you to confirm that you want to remove that version and reboot your PC. (See Figure 5-29.)

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls:
Doc: 3701

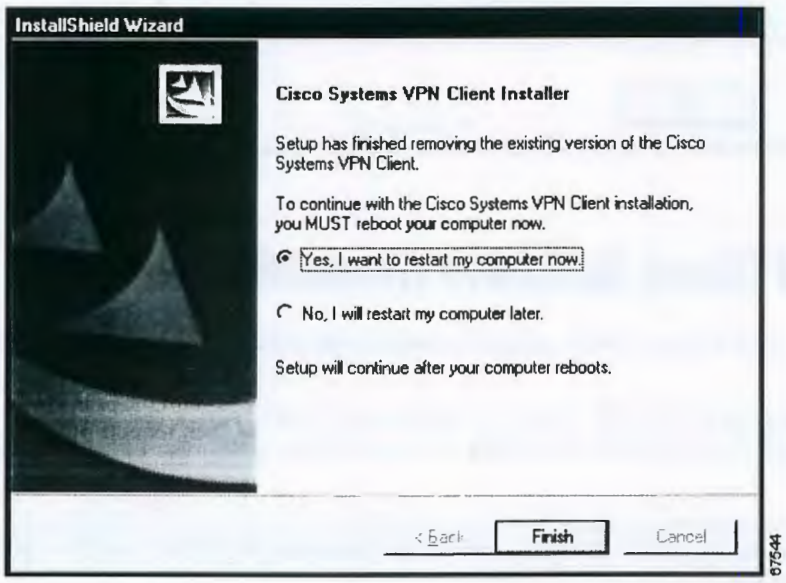
Figure 5-29 Uninstalling an Existing Version



Step 2 To continue, click **Yes**.

The installation program removes the old version and asks you to confirm the system restart. (See Figure 5-30.)

Figure 5-30 Confirming the System Restart



Be sure to remove any diskette from its drive before you restart your system.

If you are installing from diskettes, reinsert Disk 1 after your system restarts and displays the Windows logo screen, but *before* the desktop appears.

Step 3 To restart your system, click **Yes** (the default) and click **Finish**.

The installation wizard restarts your system. Once your system has restarted, installation continues automatically.

Step 4 Follow the instructions as if you were installing for the first time. See "Installing the VPN Client Through InstallShield."

4.440
J

Upgrading the VPN Client Software (MSI)

Upgrading the VPN Client software using this MSI in this recommended way retains existing connection entries and their parameters.

To install an upgrade of the VPN Client over an existing version on your system, use the following procedure.

Step 1 Remove any existing version of the VPN Client software through the Add/Remove available from the Windows Control Panel.

Step 2 Install the VPN Client using the MSI installer (vpnclient_en.msi).

Uninstalling the VPN Client with the Uninstall Application

This option is available only if you have installed the VPN Client via InstallShield. Uninstalling the VPN Client means completely removing all VPN Client software from your computer. For example, if you are changing or upgrading your PC, you might want to uninstall the VPN Client. Also, if you are getting ready to install Cisco VPN Client 3.6 using Microsoft Windows Installer (MSI), you can run the Uninstall application to remove previous versions of the Cisco VPN Client.

Note Do not attempt to uninstall or upgrade the VPN Client software from a mapped network drive.

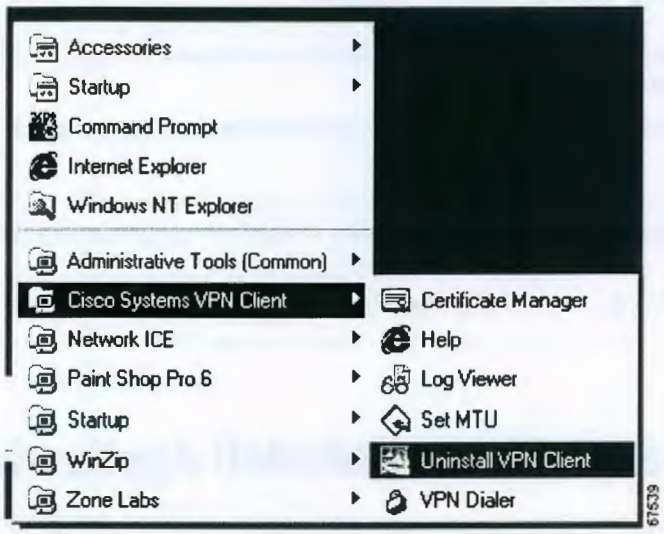
Before you run the uninstall program, make sure you have closed all of your remote access (Dial-Up Networking) connections and all VPN Client applications. Then use the following procedure. (See Figure 5-31.)

Note If you installed the VPN Client via the Microsoft Windows Installer, the Cisco Systems VPN Client menu does not include the Uninstall VPN Client option.

Step 1 Choose **Start > Programs > Cisco Systems VPN Client > Uninstall VPN Client.**

RQS Nº 03/2005 - CN -
GPMI - CORREIOS
0992
Fls:
3701
Doc:

Figure 5-31 Running the Uninstall Program



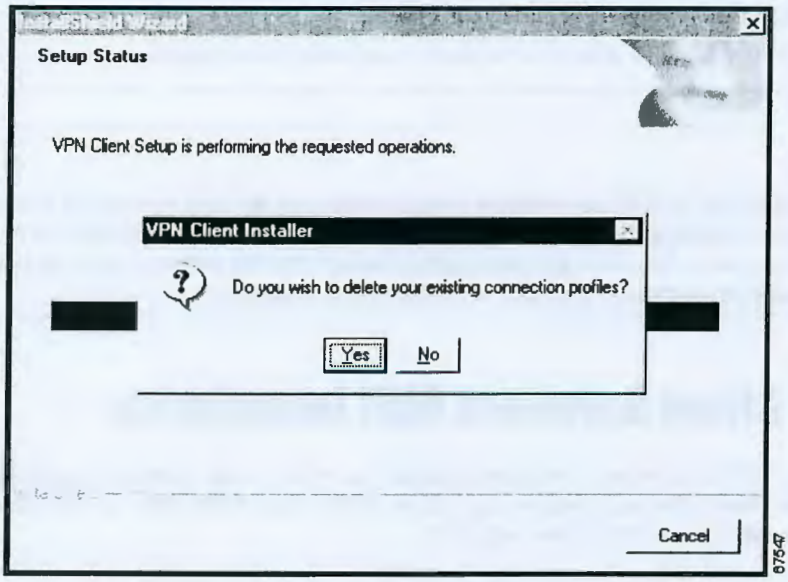
The Uninstall Wizard runs and asks if you want to really want to remove the VPN Client applications. (See Figure 5-32.)

Figure 5-32 Confirming Uninstall

Step 2 To completely remove the VPN Client software from your system, click **Yes**. Otherwise, click **No**.

Next, the Uninstall Wizard asks if you want to delete your connection profiles. (See Figure 5-33.)

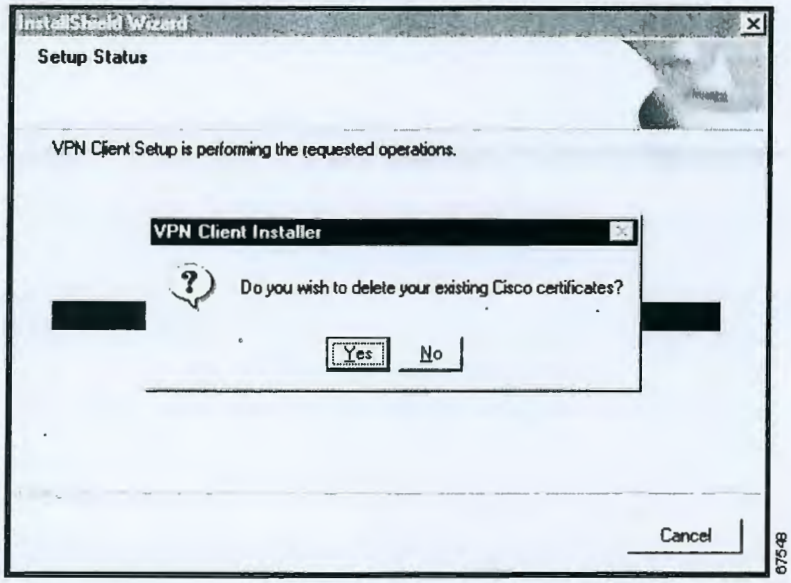
Figure 5-33 Confirming Your Connections



Step 3 To preserve your connection profiles (which contain configured connection entries), click **No**.

Then the Uninstall Wizard asks if you want to delete your certificates. (See Figure 5-34.)

Figure 5-34 Confirming Your Certificates



Step 4 To keep your certificates, click **No**.

Finally, the Uninstall Wizard prompts you to restart your system. To complete the uninstallation, you must restart your system.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0993
Fls:
Doc: 3701

Step 5 To restart your system, click **Yes** (the default) and then click **Finish**.

The installation program restarts your system.

Be sure to remove any diskette from its drive before you restart your system.

Note When you uninstall the VPN Client software after you have run the Log Viewer and you have clicked yes to remove your certificate and profile directories, the vpnclient.ini and ipseclog.txt files remain on your system. Since these files were generated after you installed the software, they are not removed when you uninstall the software. You have to remove them manually.

Removing the VPN Client Software MSI Installation

To remove the VPN Client when it has been installed via MSI, use the Add/Remove utility available from the Control Panel. You must remove any version of the Cisco VPN Client or any other VPN Client before upgrading the Cisco VPN Client with MSI.

CHAPTER 6

Enrolling and Managing Certificates

This chapter explains how to enroll and manage personal certificates using the Certificate Manager application. Specifically, it describes how to perform the following tasks:

- Obtain personal certificates through enrollment with a Certificate Authority (CA), which is an organization that issues digital certificates that verify that you are who you say you are.

  You can enroll for a certificate in two ways:

  - through the network (*online enrollment)*
  - through a file
- Import certificates
- Manage certificates
  - Viewing
  - Verifying
  - Deleting
  - Exporting
- Manage enrollment requests

This chapter covers the following topics:

- Starting Certificate Manager
- What are Certificate Stores?
- Enrolling for a Certificate
- Managing Personal and CA/RA Certificates
- Managing Enrollment Requests

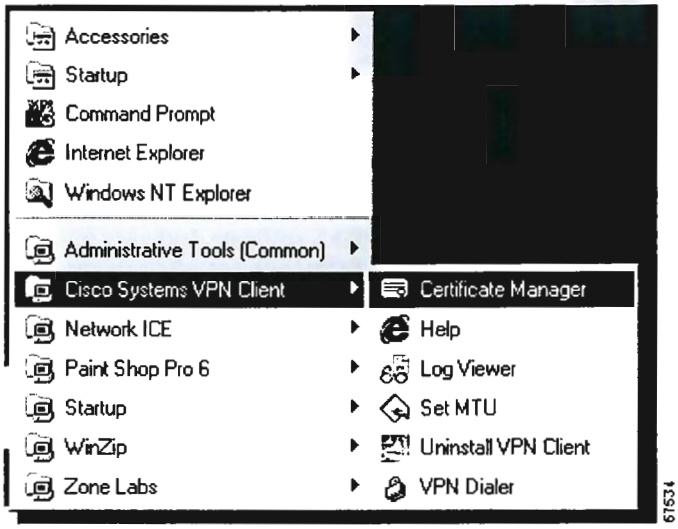
RQS Nº 03/2005 - CN
CPMI - CORREIOS
0994
Fls:
Doc: 3701

Starting Certificate Manager

To get started with certificates, go to the Cisco Systems VPN Client menu (the same menu that you use to start the client, shown in Figure 6-1).

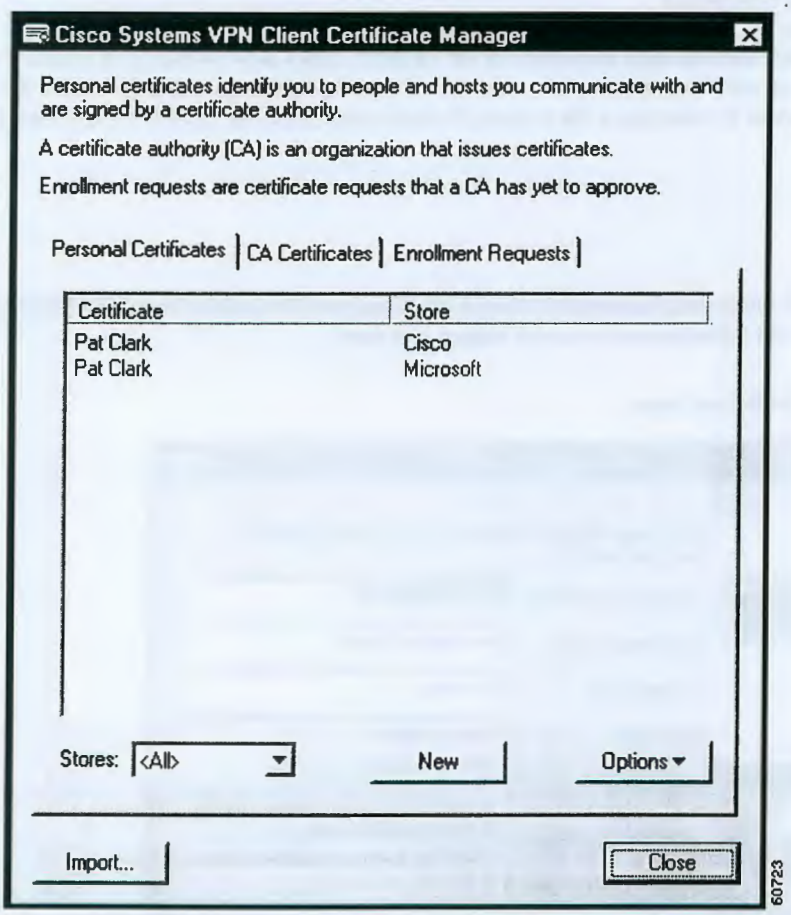
Choose **Start> Programs> Cisco Systems VPN Client> Certificate Manager.**

Figure 6-1 Choosing Certificate Manager



The Certificate Manager window opens. (See Figure 6-2.)

Figure 6-2 Certificate Manager Main Window



What are Certificate Stores?

The Certificate Manager uses the notion of *store* to convey a location in your local file system for storing personal certificates. The major store for the VPN Client is the Cisco store. The Cisco store contains certificates you have enrolled for through the Simple Certificate Enrollment Protocol (SCEP). This application supports several standard enrollment protocols. Your system also includes a Microsoft certificate store that may contain certificates that your organization provides or that you have installed previously. You can manage them just like the certificates in your Cisco store, or you can import them to your Cisco store. New certificates obtained through enrollment or importing go into the Cisco store.

There are two types of Microsoft certificates: certificates for individuals to use and also a Microsoft certificate for your local PC itself. So if several people are using the same PC, each person can have a certificate, and there can also be a certificate for the local system on Windows 2000 and Windows XP. On a Windows 9x system, you can only use it with Internet Explorer version 5.1 SP2.

Microsoft certificates with non-exportable private keys are also available.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 0995
Doc:

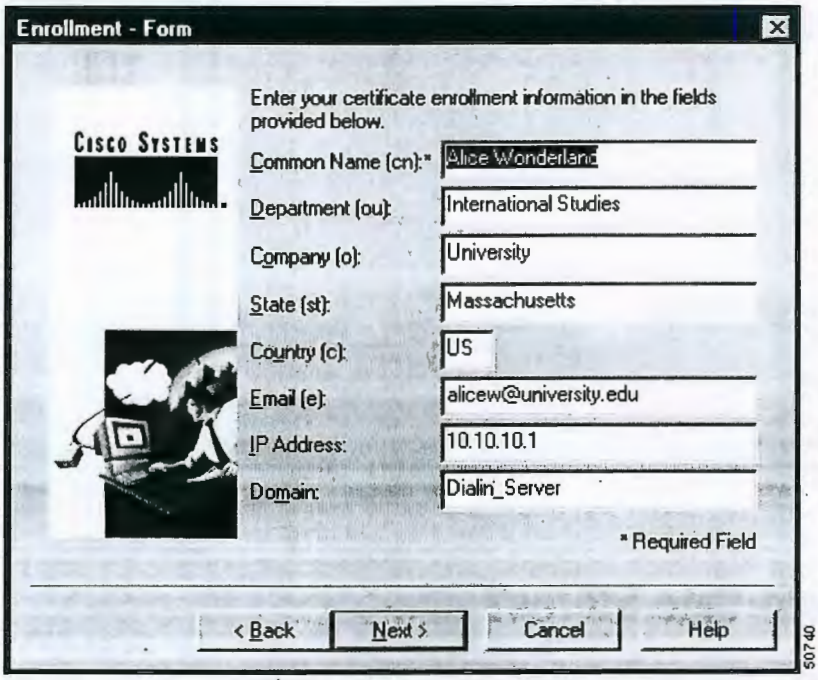
Enrolling for a Certificate

Your system administrator may have already set up your VPN Client with digital certificates. If not, or if you want to add certificates, you can obtain a certificate by enrolling with a Certificate Authority (CA) over the network or by creating a file request. In both cases, you complete the same form (shown in Figure 6-3.)

Enrollment Form

This section describes the information required for filling out the certificate enrollment form. Make sure you have all of the following information before you start.

Figure 6-3 Enrollment Form



- Common Name—Your common name (CN), which is the unique name to use for this certificate. This field is required. The common name can be the name of a person, system, or other entity; it is the most specific level in the identification hierarchy. The common name becomes the name of the certificate; for example, Alice Wonderland.
- Department—The name of the department to which you belong; for example, International Studies. This field correlates to the Organizational Unit (OU). The OU is the same as the Group Name configured in a VPN 3000 Series Concentrator, for example.
- Company—The name of the company or organization (O) to which you belong; for example, University.
- State—The name of your state (ST); for example, Massachusetts.

- Country—The 2-letter country code for your country (C); for example, US. This two-letter country code must conform to ISO 3166 country abbreviations.
- Email—Your email address (e); for example, alicew@university.edu.
- IP Address—The IP address of your system, for example, 10.10.10.1.
- Domain—The Fully Qualified Domain Name of the host for your system; for example, `Dialin_Server`.

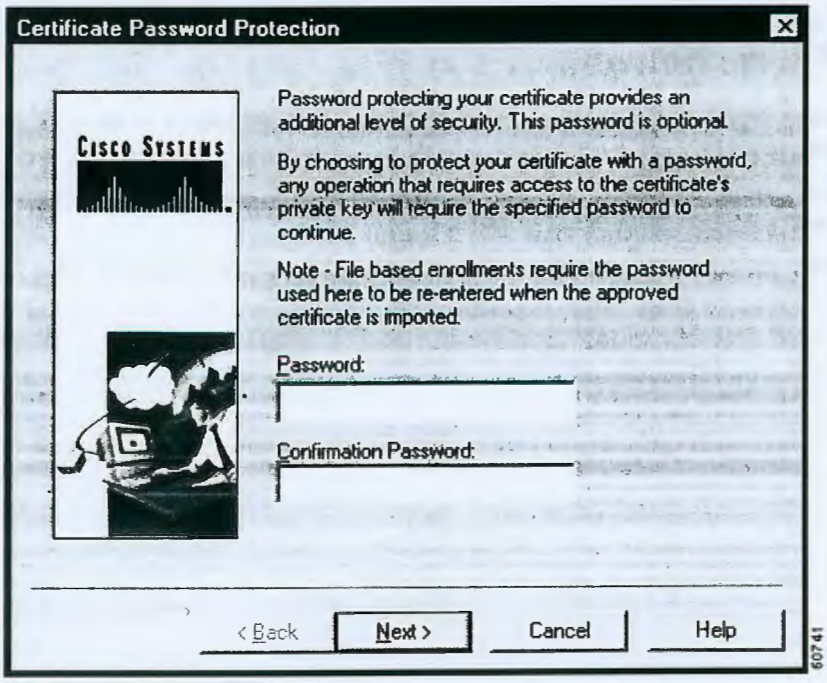
Together, all these fields except IP address and domain comprise your distinguished name (DN).

When you enroll a personal certificate, either you go through a CA from which your system already has a root certificate or you obtain a root certificate from the CA as part of the enrollment process. The CA Certificates tab displays the current list of CA certificates. (See Figure 6-2.)

Starting Enrollment

To begin, click **New** on the Certificate Manager's main screen under the Personal Certificates tab. (See Figure 6-2.) The Certificate Manager prompts you to enter a password for the certificate you are enrolling. (See Figure 6-4.) The password is optional, but we recommend that you use one to protect your private key more effectively. The password can be up to 32 characters in length. Passwords are case sensitive. For example, *sKate8* and *Skate8* are different passwords. This password is called the *personal certificate password*.

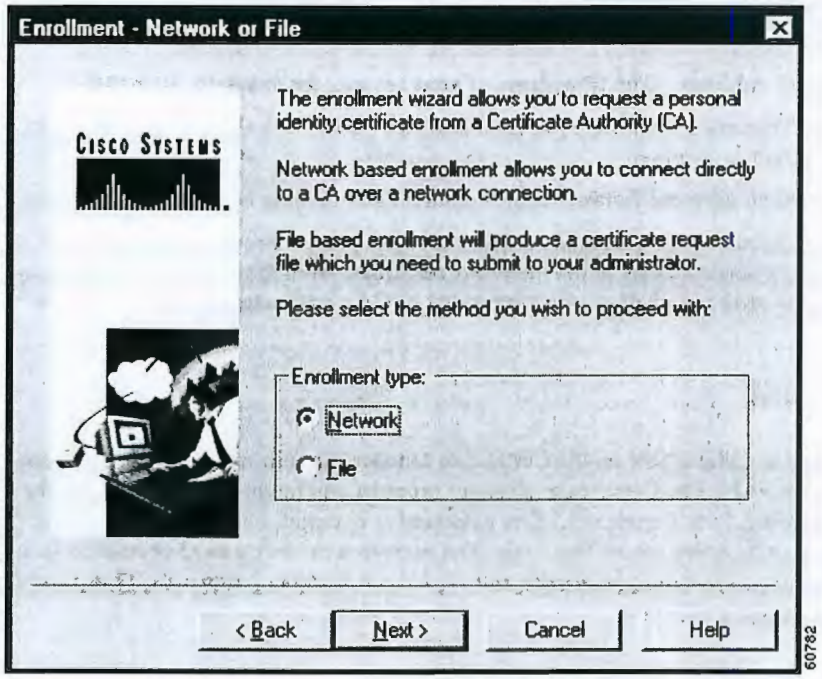
Figure 6-4 Protecting a Certificate with a Password



After entering a password, click **Next** to continue. The Certificate Manager lets you choose between enrolling via the network or by creating a file. (See Figure 6-5.) Enrolling via the network is also called *online enrollment*.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
0996
Fls:
Doc: 3701

Figure 6-5 Choosing Enrollment Method



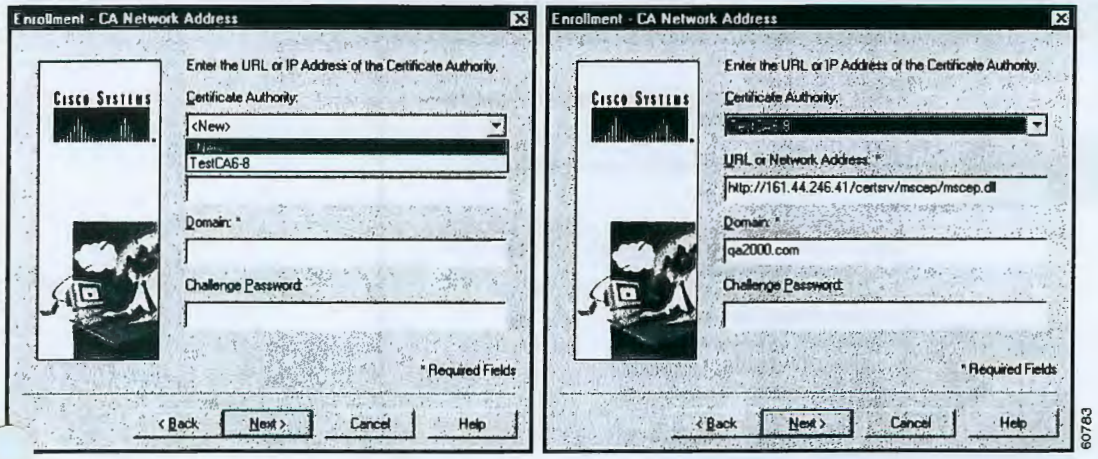
Enrolling Through the Network

To enroll through the network, retrieve a certificate from a CA, and place it in the Cisco store, using the following procedure:

Step 1 Click **Network** and click **Next**. (See Figure 6-5.)

The Certificate Manager asks you to enter the network address of the issuing CA. (See Figure 6-6.)

Figure 6-6 Entering Network Address



Step 2 Choose one of the following procedures:

- Choose an existing Certificate Authority from the drop-down menu.
  - The URL or Network Address and Domain fields are automatically filled.
  - Renter the Challenge password or enter a new password, which you can obtain from the CA or your network administrator.
- Choose **<New>** from the drop-down menu.
  - Enter the URL or Network Address of the CA and the CA's Domain, both of which are required.
  - Some CAs require that you enter a password to access their site. If this is the case, enter the password in the Challenge Password field. You can get the password from the CA or from your network administrator.

Step 3 When you have completed the network address information, click **Next**.

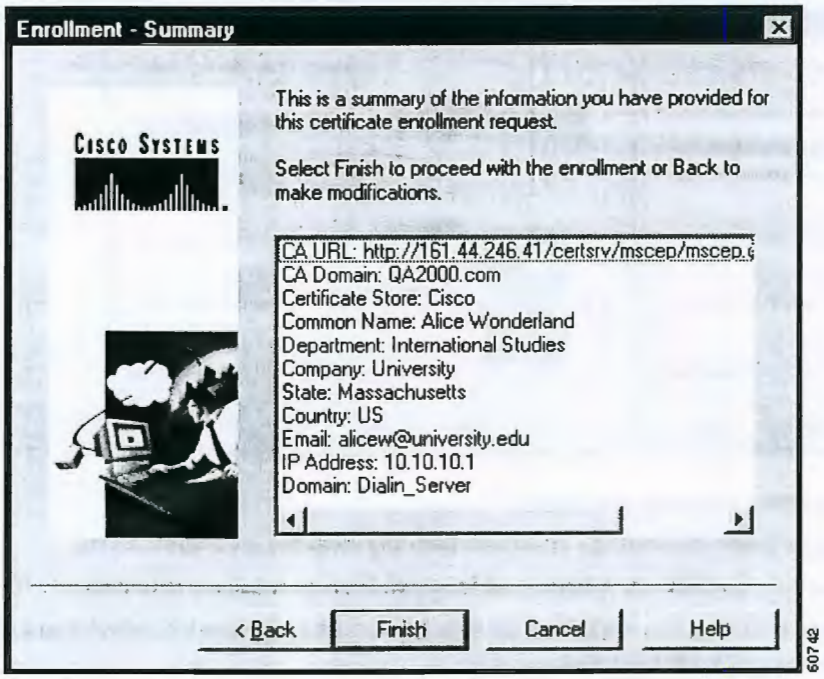
The Certificate Manager displays the enrollment form for you to complete. (See Figure 6-3.)

Step 4 Enter the information you collected before you started the enrollment process. The only field that the Certificate Manager requires is Common Name. However the CA may require some or all of the other fields. Then click **Next**.

After you enter the form, the Certificate Manager displays a summary that looks something like the one in Figure 6-7.

4430
RQS Nº 03/2005 - CN
CPMI - CORREIOS
0997
Fls:
3701
Doc:

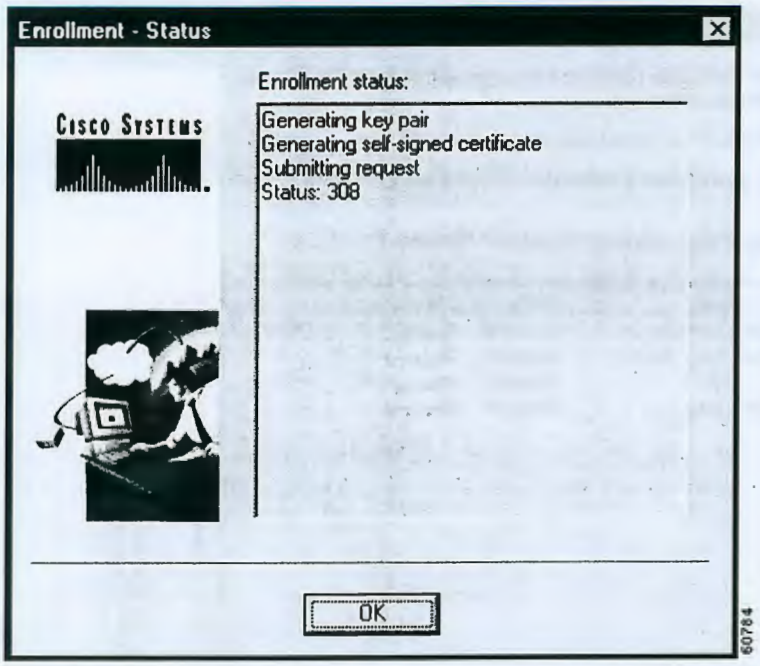
Figure 6-7 Enrollment Summary



Step 5 To complete the enrollment, click **Finish**.

The Certificate Manager displays a status window (shown in Figure 6-8) that lets you monitor the progress of the certificate retrieval. If the enrollment failed, the status window indicates the cause so you can fix the problem and try again.

Figure 6-8 Certificate Status Messages

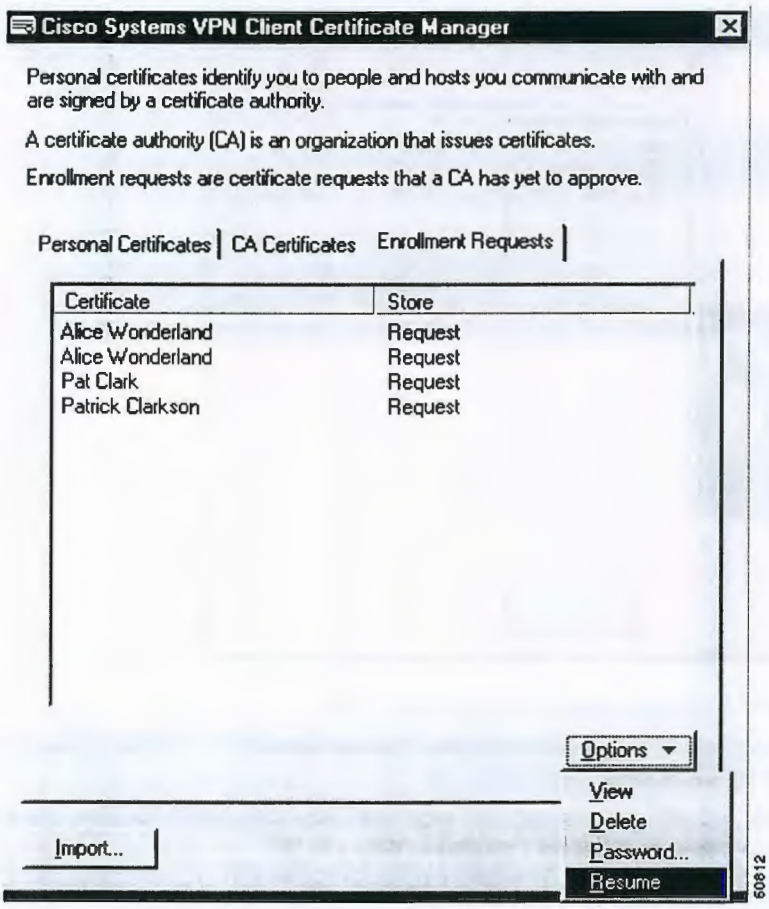


Step 6 What happens next depends on your CA. (See Figure 6-8):

- Some CAs may provide immediate response. If so, the Enrollment - Status window reflects this fact and displays an OK button.
  - Click **OK** and you see a message that your enrollment succeeded. You can view and manage the certificate under the Personal Certificates tab.
- If the enrollment status is Request pending, your CA does not immediately approve your request and the Enrollment - Status window shows the Suspend button.
  - Click **Suspend**.
  - Your request appears under the Enrollment Requests tab, while you are waiting for the CA to issue the certificate.
  - When the CA issues your certificate, choose the certificate and then choose **Resume** from the Options pull-down menu to complete the enrollment. (See Figure 6-9.)

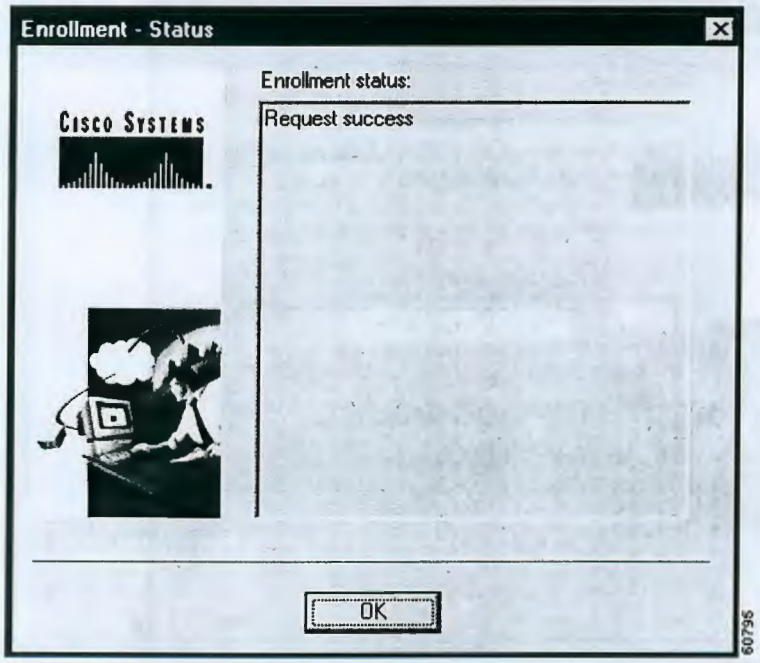
RQS Nº 03/2005 - CN
CPMI - CORREIOS
0998
Fls:
3701
Doc:

Figure 6-9 Resuming Enrollment Request



- After you have obtained the certificate, the status screen updates to show the result. (See Figure 6-10.) After viewing the screen, click **OK**.

Figure 6-10 Receiving Status Update



Enrolling Through a File Request

Alternatively, you can enroll by creating a file using the same form as network enrollment. (See Figure 6-3.) Once you have created a request file, you can either e-mail it to the CA and receive a certificate back or you can access the CA's website and cut and paste the enrollment request in the area that the CA provides.

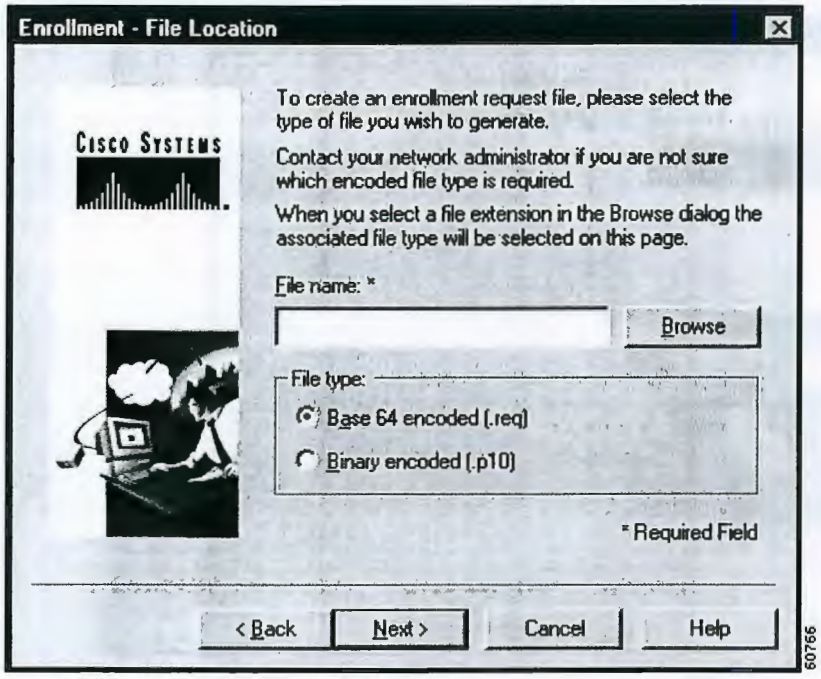
To enroll through a file request, use the following procedure:

Step 1 At the Enrollment - Network or File dialog box. (See Figure 6-5), click **File** and click **Next**.

The Certificate Manager prompts you to choose a file type for your file request and to specify a file name. (See Figure 6-11.)

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 0999
Doc: 3701

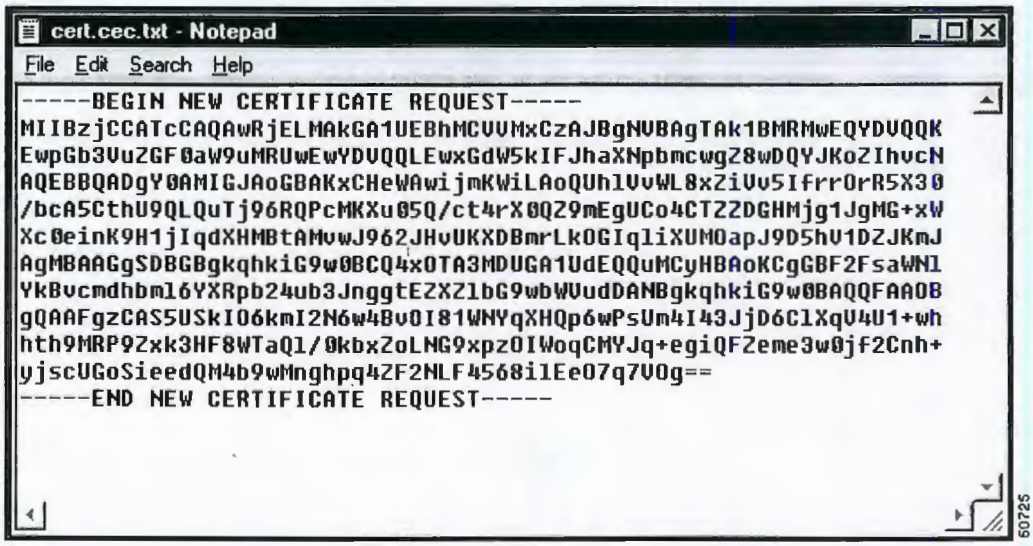
Figure 6-11 Choosing file type and location



Step 2 Click one of the following file types:

- **Binary encoded**—A base-2 PKCS10 file (Public Key Cryptography Standard; for example, an X.509 DER file). You cannot display a binary-encoded file.
- **Base 64 encoded**—An ASCII-encoded PKCS10 file that you can display in text format (for example, the request shown in Figure 6-12). Choose this type when you want to cut and paste the text into the CA website.

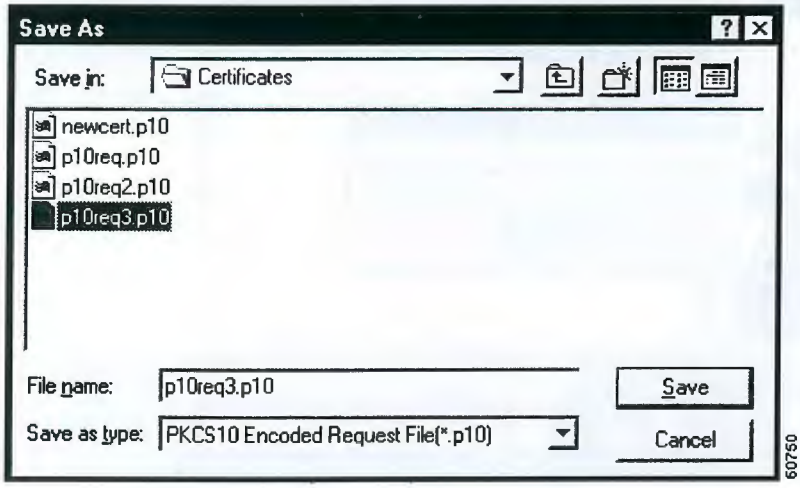
Figure 6-12 A PKCS10 Certificate Request



Step 3 Enter the full pathname for the file request.

When you browse for an appropriate directory for placing the file request, the Certificate Manager shows only the files of the chosen file type. (See Figure 6-13.) You can save your file enrollment requests in the Certificates directory, which is a subdirectory of the directory where the VPN Client is installed.

Figure 6-13 Specifying a Filename



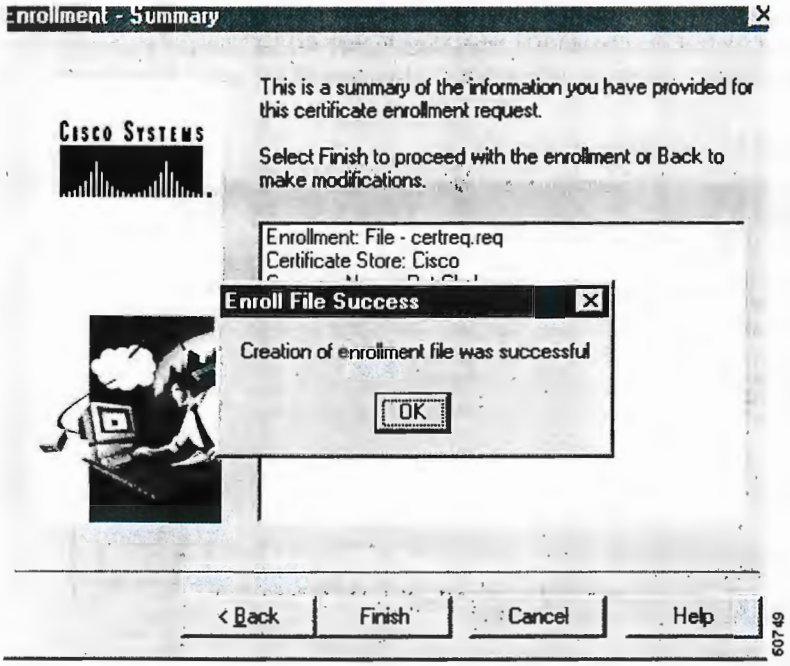
In this example, the complete pathname is C:\Program Files\Cisco Systems\VPN Client\Certificates\p10req3.p10.

Step 4 Complete the form (see the "Enrollment Form" section) and click **Next**.

The Certificate Manager displays the summary screen and a message to let you know that your request succeeded. (See Figure 6-14.)

4.424
RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1000
Doc: 3701

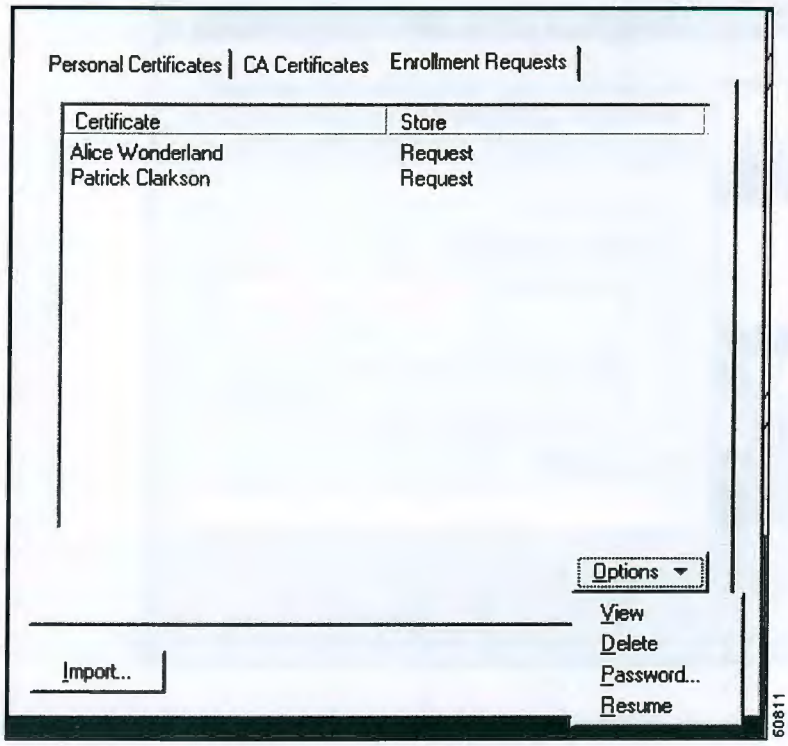
Figure 6-14 Enroll File Success Message



Step 5 Click **OK** on the message screen then click **Finish** on the summary screen.

You can view the file request under the Enrollment Requests tab. (See Figure 6-15.)

Figure 6-15 File Enrollment Requests



Importing a Certificate File

You can import a certificate into the Cisco store from the Microsoft store or from a file. To import a certificate, use the following procedure:

Step 1 On the Certificate Manager main window under the Personal Certificates tab, click **Import**.

The Certificate Manager displays the Import Certificate - Source dialog box. (See Figure 6-16.)

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1001
Doc: 3701

Figure 6-16 Importing a Certificate

Step 2 To import a certificate, do one of the following, depending on where your certificate resides:

- Importing from the Microsoft store—Click **Microsoft certificate** and choose the certificate from the drop-down menu. The certificate must already be in your Microsoft store.
- Importing from a file—Click **File** and enter the pathname of the file into the field.

Step 3 If a password is used to protect this certificate, type the password into the Import Password: field.

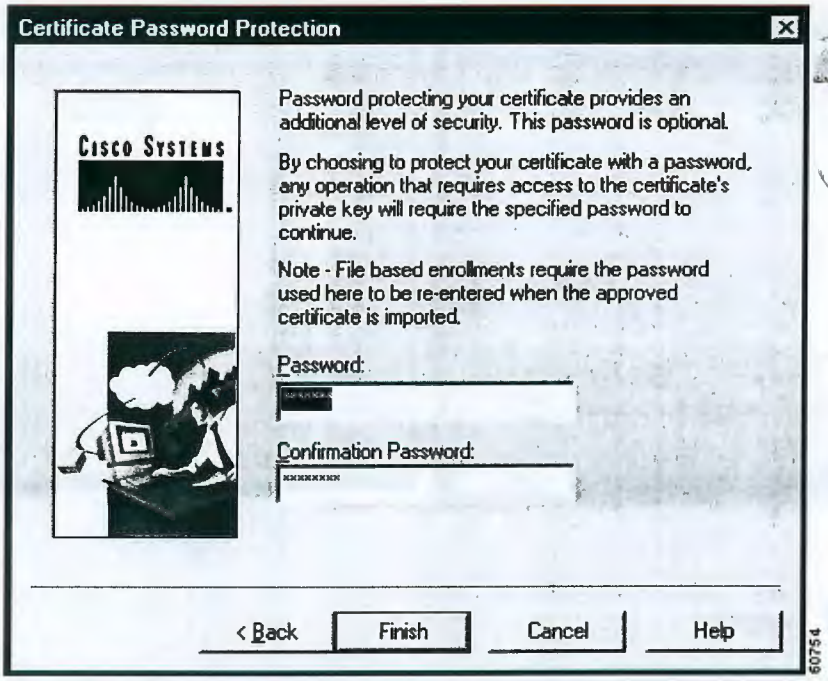
This is the password assigned to protect the certificate's private key.

- If you are importing from the Microsoft store, this password is the one you (or the network administrator) entered during enrollment.
- If you are importing a certificate from a file, this is the password specified when the certificate was exported.

Step 4 Click **Next**.

The Certificate Manager prompts for a password to be stored with the certificate. (See Figure 6-17.)

Figure 6-17 Destination Password for Importing Certificate



Step 5 Type a password into the Password field, and click **Finish**.

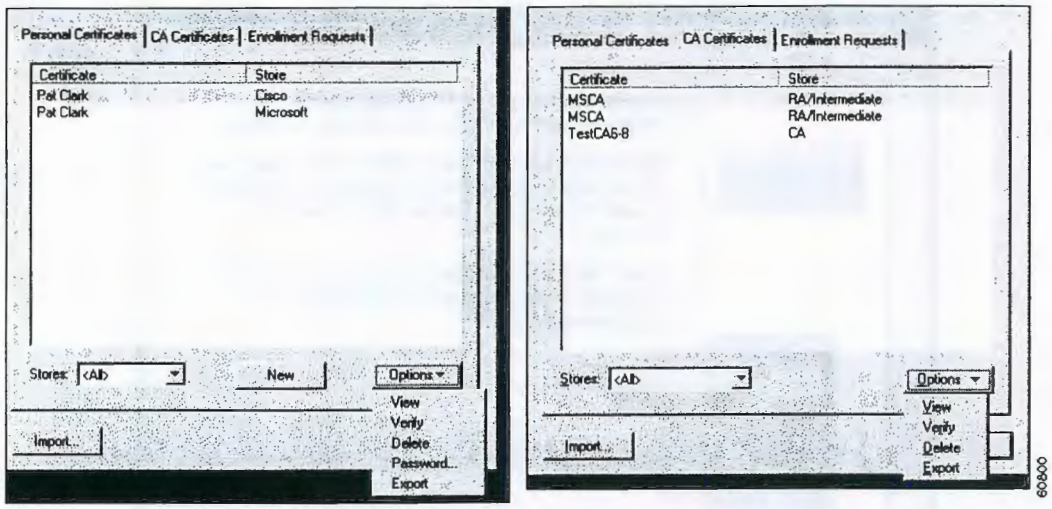
This password must exactly match the password given during enrollment (online) or given when exported (if a file), including upper and lower case letters. For example, *sKate8* is not exactly the same as *Skate8*. In online enrollment, this password is kept with the certificate; in file enrollment, this password is not retained.

Managing Personal and CA/RA Certificates

Using the Certificate Manager, you can view a certificate, verify that the certificate is still valid (within the dates assigned to it and has not been revoked), delete a certificate, and export the certificate to a file that you can e-mail. For personal certificates only, you can also change the certificate password. To perform any of these actions, use the Options menu on the main window. (See Figure 6-18.)

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1002
Fls:
3701
Doc:

Figure 6-18 Certificate Manager Options Menu



Viewing a Certificate

To display a certificate, choose it in the certificate store, open the Options pull-down menu and choose **View**. Or, you can double-click on the certificate to display it.

Figure 6-19 shows a sample certificate from a Microsoft certificate service provider. This is only an example. Not all certificates are guaranteed to look like this one.

Figure 6-19 Displaying a Certificate

A typical certificate shown in Figure 6-19 contains the following information.

- Common Name—The name of the owner, usually the first name and last name. This field identifies the owner within the Public Key Infrastructure (PKI organization).
- Department—The name of the owner's department, which is same as the Organizational Unit (OU). Note that when connecting to a VPN 3000 Concentrator, the OU should generally match the Group Name configured for the owner in the VPN 3000 Concentrator.
- Company—The organization where the owner is using the certificate.
- State—The state where the owner is using the certificate.
- Country—The two-character country code where the owner's system is located.
- Email—The email address of the owner of the certificate.
- Key Size—The size of the signing key pair in bits; for example, 1024.
- Subject—The fully qualified distinguished name (DN) of certificate's owner. This specific example includes the following parts. Other items may be included, depending on the certificate type. However, these fields are fairly standard.
  - cn is the common name.
  - ou is the organizational unit (department)
  - o is the organization
  - l is the locality (city or town).

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1003
Doc: 3701

  - st is the state or province of the owner.
  - c is the country.
  - e is the email address of the owner.
- Issuer—The fully qualified distinguished name (DN) of the source that provided the certificate. The fields in this example are the same as for Subject.
- Serial Number—A unique identifier used for tracking the validity of the certificate on Certificate Revocation Lists (CRLs).
- Not Before—The beginning date that the certificate is valid.
- Not After—The end date beyond which the certificate is no longer valid.

The next three fields may be used during a connection attempt as part of validation, for example, to make sure that the Subject Alternative IP Address matches the IP Address of the VPN Concentrator.

- Alt Name DNS—The name of the Domain Name Server for the Subject Alternative Name.
- Alt Name Email—The email address of the Subject Alternative Name.
- Alt Name IP Addr—The IP address of the Subject Alternative Name.

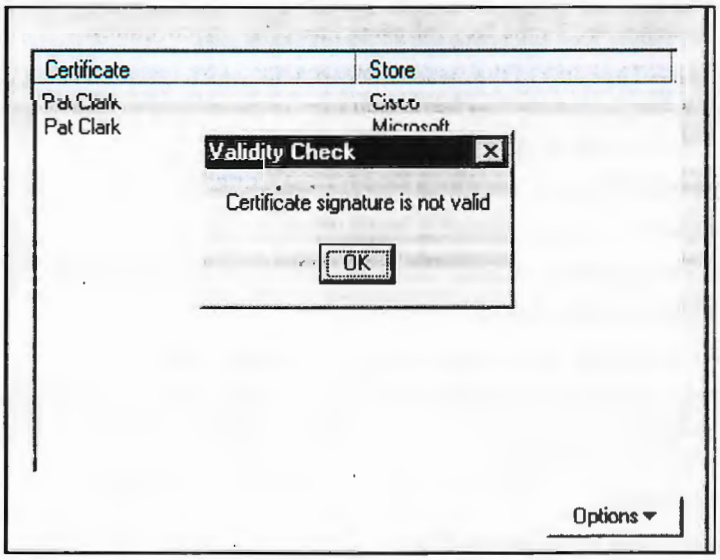
After you have finished viewing the certificate, click **OK** to close it.

Verifying a Certificate

The Certificate Manager provides a quick way for you to check the validity of a certificate; for example, to see if it is within the valid beginning and ending date range. To see if the certificate is valid, choose it in the certificate store, display the Options pull-down menu, and choose **Verify**.

The Certificate Manager displays a message such as the one in Figure 6-20 indicating whether the certificate is still valid.

Figure 6-20 Verifying a Certificate's Validity



ECT 14.436 ECT - AC

The following table shows the messages you might see when you check the validity of your certificate:

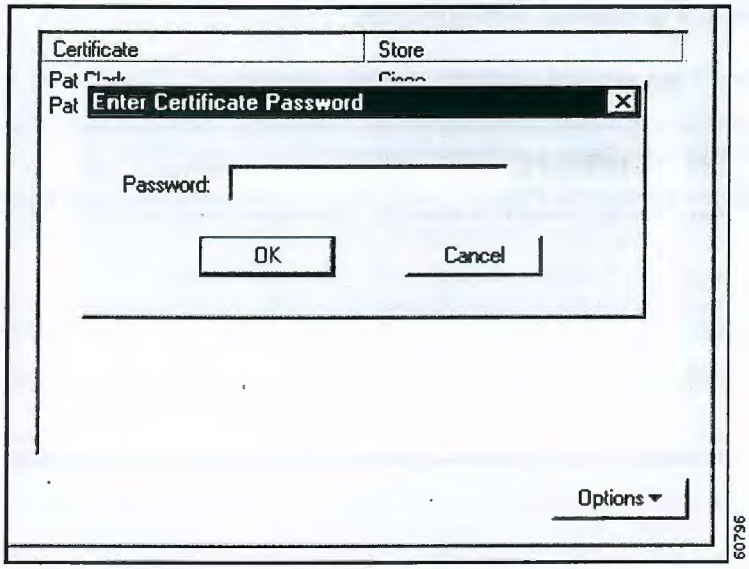
Message	Description
`Certificate is not valid yet`	The current date is prior to the certificate's valid start date. You must wait until the certificate becomes valid.
`Certificate has expired`	The current date is after the certificate's valid end date. You need to enroll for a new certificate.
`Certificate signature is not valid`	You do not have the CA certificate, or the CA certificate that you have may have expired. You might need to download or import the CA certificate.
`Certificate is valid`	You have a working certificate enrolled.

Deleting a Certificate

To delete a certificate, follow this procedure:

Step 1 Choose the certificate in the certificate store, display the Options pull-down menu, and choose **Delete**. If the certificate has a password, the Certificate Manager prompts you to enter it. (See Figure 6-21.)

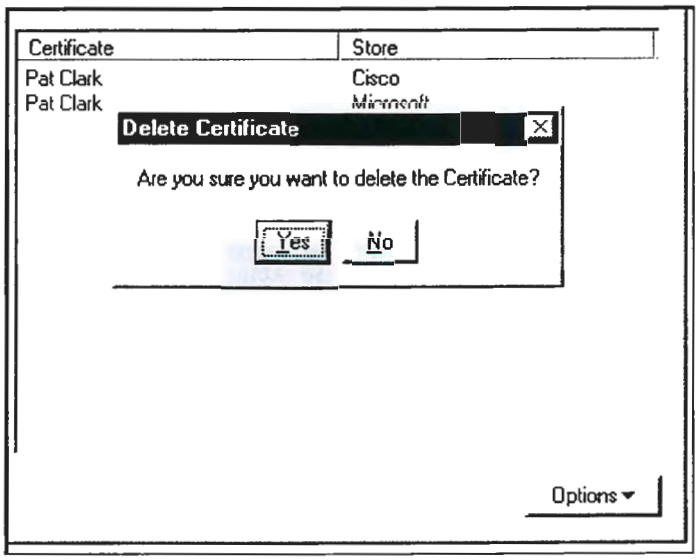
Figure 6-21 Entering Password for Deleting a Certificate



Step 2 In the Password field, type the password given to the certificate during enrollment and click **OK**. Next, the Certificate Manager asks you to confirm. (See Figure 6-22.)

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1004
Doc: 3701

Figure 6-22 Confirming Deletion



Step 3 To complete the deletion, click **Yes**. If you decide not to delete this certificate, click **No**.

Changing the Password on a Personal Certificate

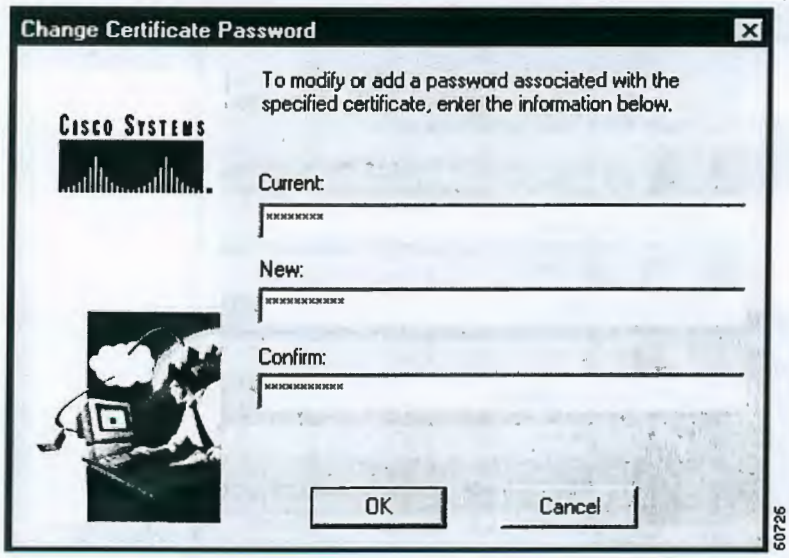
To change the password on a personal certificate, use this procedure:

Step 1 Display the Options pull-down menu and choose **Password...**.

The Certificate Manager displays the Change Certificate Password dialog box. (See Figure 6-23.)

ECT 4.414 J CPL - AC

Figure 6-23 Changing a Certificate Password



Step 2 In the Current field, type the password you are currently using to protect your private key.

Step 3 In the New field, type the new password.

Step 4 In the Confirm field, type the same password again.

Step 5 Click **OK**.

Exporting a Certificate

You may want to export a certificate, primarily for backing up your certificate and private key or moving them to another system. When you export a certificate, you are making a copy of it.

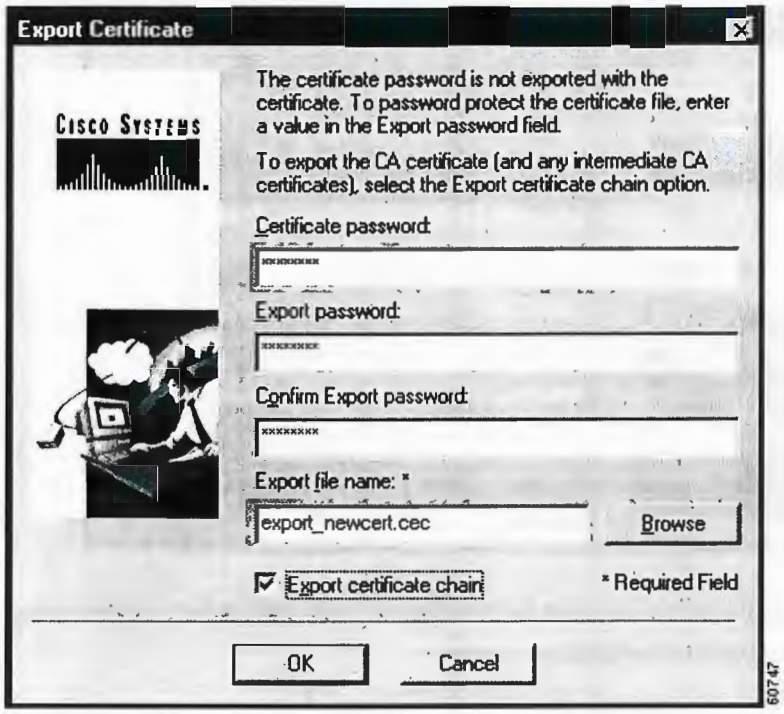
To export a certificate, follow these steps:

Step 1 Display the Options pull-down menu and choose **Export**.

The Certificate Manager displays the Export Certificate dialog box. (See Figure 6-24.)

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1005
Doc: 3701

Figure 6-24 Exporting a Certificate



Step 2 In the Certificate password field, enter the password initiated during enrollment.

The Certificate password protects the certificate in the certificate store (so an unauthorized individual can not use it). This is the password you *optionally* entered when you enrolled for the certificate.

Step 3 In the Export password field, enter an optional password to protect the export file. Then enter it again in the Confirm password field.

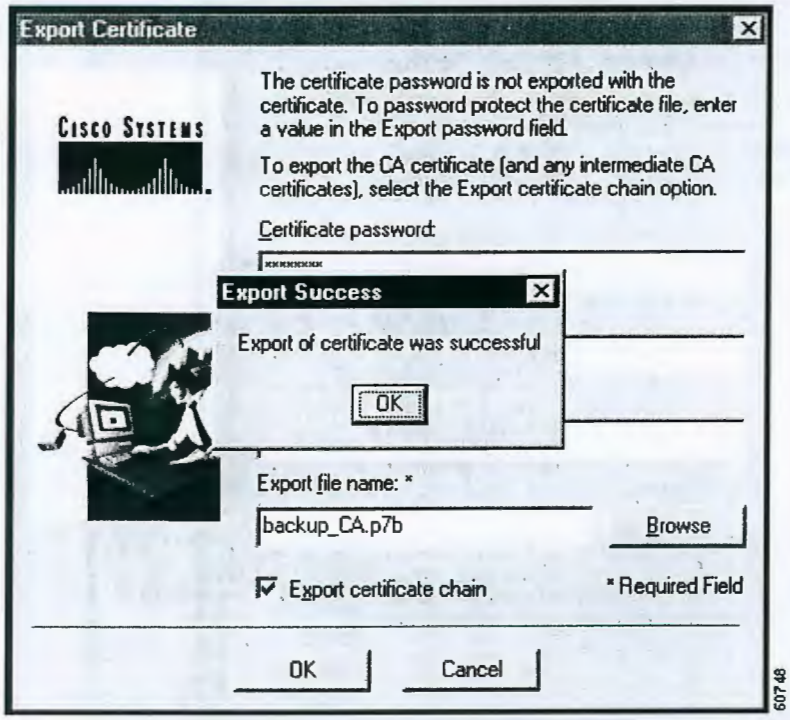
Step 4 In the Export filename field, enter the filename for the exported certificate. Only the filename is required. Use the Browse feature to locate a target directory for the exported certificate.

Step 5 To export the CA and/or RA certificate with your personal certificate, check the **Export certificate chain** option.

Step 6 After completing all the information, click **OK**.

The Certificate Manager displays a message indicating whether your certificate export was successful. (See Figure 6-25.)

Figure 6-25 Export Message



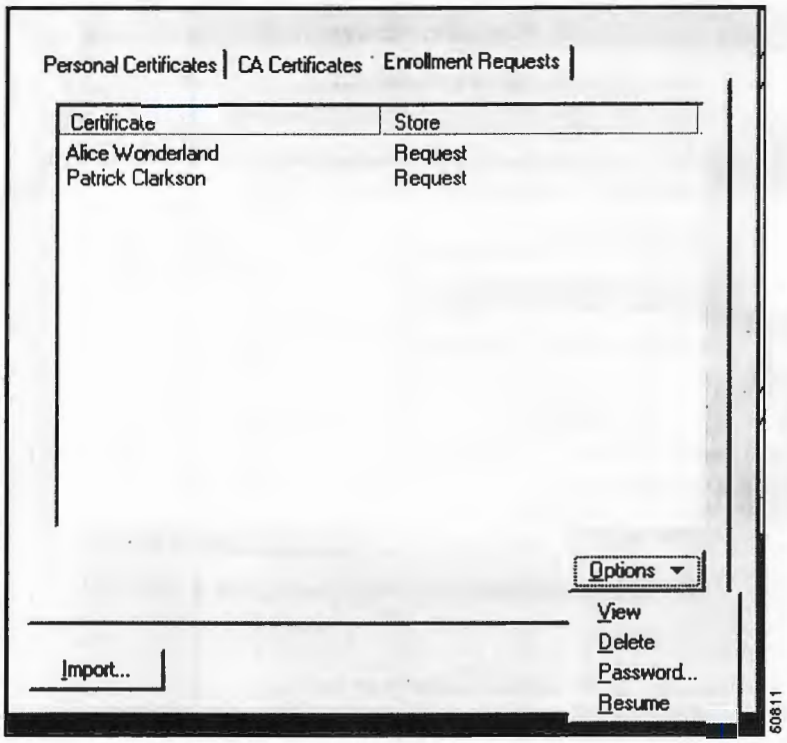
Step 7 To continue, click **OK**.

Managing Enrollment Requests

While a request is pending approval by the CA administration, the Certificate Manager places the enrollment request under the Enrollment Requests tab. You can view, delete, or change the password on any request in the list; or you can resume a network enrollment request. To perform any of these actions, choose the Enrollment Requests tab and click on the Options pull-down menu. (See Figure 6-26.)

ECT 4.412 J C.L. - A.C.
RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1006
Doc: 3701

Figure 6-26 Managing Enrollment Requests



Viewing the Enrollment Request

To display the enrollment request, click on its name in the list and choose **View** from the Options pull-down menu. The Certificate Manager displays the pending request. (See Figure 6-27.)

Figure 6-27 Viewing an Enrollment Request

Note that the Issuer field shows the subject name and not the name of the CA, since the CA has not yet issued the certificate.

Deleting an Enrollment Request

To delete an enrollment request, follow these steps:

Step 1 Click on the enrollment request in the list and choose **Delete** from the Options pull-down menu.

The Certificate manager prompts you for a password.

Step 2 Type the password in the Password field and click **OK**.

The Certificate Manager verifies the password. If the password is correct, the Certificate Manager asks you to confirm that you really want to delete the enrollment request.

Step 3 To complete the deletion, click **Yes**. If you decide not to delete this certificate, click **No**.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1007
Fls:
Doc: 3701

Changing the Password on an Enrollment Request

To change the certificate password on an enrollment request, use this procedure:

Step 1 Display the Options pull-down menu and choose **Password**.

The Certificate Manager displays the Change Certificate Password dialog box. (See Figure 6-28.)

Figure 6-28 Changing a Certificate Password

Step 2 In the Current field, type the password you are currently using.

Step 3 In the New field, type the new password.

Step 4 In the Confirm field, type your new password again.

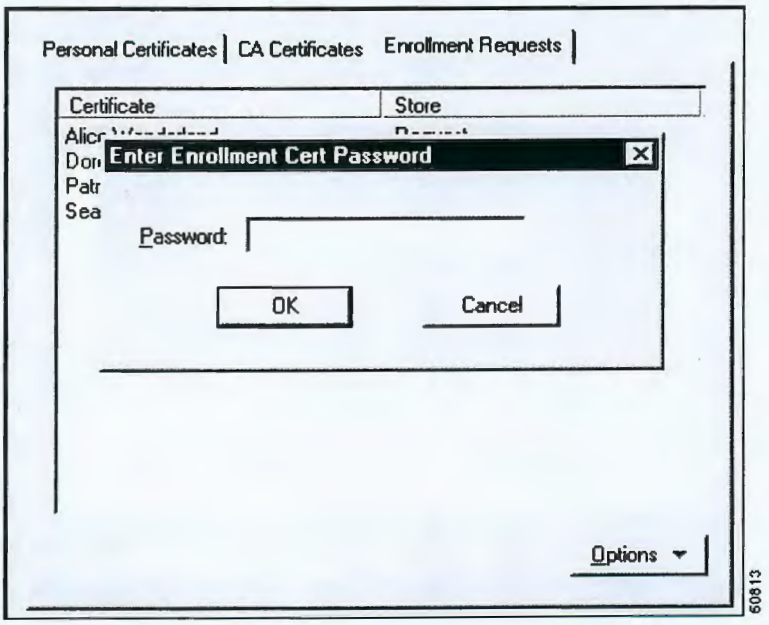
Step 5 Click **OK**.

Completing an Enrollment Request

To complete a pending enrollment request, choose the request under the Enrollment Requests tab, and choose **Resume** from the Options pull-down menu.

The Certificate Manager prompts you to enter a password. (See Figure 6-29.) This password must match the password you are using to protect the certificate's private key, if any.

Figure 6-29 Entering Password to Resume Online Enrollment



Enter the password and click **OK** to resume enrollment.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1008
Fls:
Doc: 3701

APPENDIX A

Copyrights and Licenses

Client Software License Agreement of Cisco Systems

THE SOFTWARE TO WHICH YOU ARE REQUESTING ACCESS IS THE PROPERTY OF CISCO SYSTEMS. THE USE OF THIS SOFTWARE IS GOVERNED BY THE TERMS AND CONDITIONS OF THE AGREEMENT SET FORTH BELOW. BY CLICKING "YES" ON THIS SCREEN, YOU INDICATE THAT YOU AGREE TO BE BOUND BY THE TERMS AND CONDITIONS OF THAT AGREEMENT. THEREFORE, PLEASE READ THE TERMS AND CONDITIONS CAREFULLY BEFORE CLICKING ON "YES". IF YOU DO NOT AGREE TO THE TERMS AND CONDITIONS OF THE AGREEMENT, CLICK "NO" ON THIS SCREEN, IN WHICH CASE YOU WILL BE DENIED ACCESS TO THE SOFTWARE.

Ownership of the Software

1. The software contained in the Cisco Systems VPN Client ("the Software"), to which you are requesting access, is owned or licensed by Cisco Systems and is protected by United States copyright laws, laws of other nations, and/or international treaties.

Grant of License

2. Cisco Systems hereby grants to you the right to install and use the Software on an unlimited number of computers, provided that each of those computers must use the Software only to connect to Cisco Systems products, and subject to export restrictions in paragraph 4 hereof. You may make one copy of the Software for each such computer for the purpose of installing the Software on that computer. The Software is licensed for use only with Cisco Systems products, and for no other use.

Restrictions on Use and Transfer

3. You may also make one copy of the Software solely for backup or archival purposes. To this end, you may transfer the Software to a single set of disks provided you keep the disks solely for backup or archival purposes. You may not use the backup or archival copy of the Software except in conjunction with Cisco Systems products.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1009
Fls:
3701
Doc:

4. You may copy and distribute the Software to your third party business partners and customers solely and exclusively for the purposes of accessing your Cisco VPN concentrators and thereby gaining remote access to your secure network. Each such distribution of the Software to a third party must be accompanied by a copy of this Client Software License Agreement. You may not copy or transfer the Software for any purpose, other than as specified in this Agreement, without the express written consent of Cisco. Without intending to limit the foregoing, you shall not post or otherwise make publicly available the Software to any external web site, file server, or other location to which there is unrestricted access.

5. Cisco Systems will not provide end-user support (including Technical Assistance or TAC support) to any third party that receives the Software in accordance with Section 4 hereof. You shall be responsible for providing all support to each such third party. For permitted transfers, you may not export the Software to any country for which the United States requires any export license or other governmental approval at the time of export without first obtaining the requisite license and/or approval. Furthermore, you may not export the Software in violation of any export control laws of the United States or any other country. (For reference purposes only, see the Cisco Encryption Tool Quick Reference Guide currently located at http://www.cisco.com/wwl/export/crypto/tool/stqrg.html.)

6. You may not modify, translate, decompile, disassemble, use for any competitive analysis, reverse engineer, distribute, or create derivative works from, the Software or any accompanying documentation or any copy thereof, in whole or in part.

7. The subject license will terminate immediately if you do not comply with any and all of the terms and conditions set forth herein. Upon termination for any reason, you (the licensee) must immediately destroy the Software, any accompanying documentation, and all copies thereof in your possession. You must also use commercially reasonable efforts to notify the third parties to whom you have distributed the Software that their rights of access and use of the Software have also ceased. Cisco Systems is not liable to you for damages in any form solely by reason of termination of this license.

8. You may not remove or alter any copyright, trade secret, patent, trademark, trade name, logo, product designation or other proprietary and/or other legal notices contained in or on the Software and any accompanying documentation. These legal notices must be retained on any copies of the Software and accompanying documentation made pursuant to paragraphs 2 through 4 hereof.

9. You shall acquire no rights of any kind to any copyright, trade secret, patent, trademark, trade name, logo, or product designation contained in, or relating to, the Software or accompanying documentation and shall not make use thereof except as expressly authorized herein or otherwise authorized in writing by Cisco Systems.

Limitation Of Liabilities

10. INSTALLATION AND USE OF THE SOFTWARE IS ALSO GOVERNED BY A SEPARATE LICENSE AGREEMENT BETWEEN CISCO SYSTEMS AND THE PURCHASER OF THE CISCO SYSTEMS VPN CLIENT PRODUCT. THAT SEPARATE LICENSE AGREEMENT CONTAINS A DESCRIPTION OF ALL WARRANTIES PROVIDED BY CISCO SYSTEMS FOR THE SOFTWARE. CISCO SYSTEMS PROVIDES NO WARRANTIES FOR THE SOFTWARE OTHER THAN THOSE SET FORTH IN THAT AGREEMENT, AND ASSUMES NO LIABILITIES WITH RESPECT TO USE OF THE SOFTWARE BY YOU OR ANY THIRD PARTY.

E C T
4.404
1
J
A C

RSA software

Copyright (C) 1995-1998 RSA Data Security, Inc. All rights reserved. This work contains proprietary information of RSA Data Security, Inc. Distribution is limited to authorized licensees of RSA Data Security, Inc. Any unauthorized reproduction or distribution of this document is strictly prohibited.

BSAFE is a trademark of RSA Data Security, Inc.

The RSA Public Key Cryptosystem is protected by U.S. Patent #4,405,829.

Zone Labs

Copyright (c) 1999, 2000, 2001. Zone Labs, Inc. All rights reserved.

Zone Labs, ZoneAlarm, ZoneAlarm Pro, TrueVector, and Zone Labs Integrity are trademarks of Zone Labs, Inc.

The Software is Zone Labs proprietary information. No license is granted to the source code of the Software.

No part of this publication may be reproduced, distributed or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of Zone Labs, Inc. THE SOFTWARE IS PROVIDED BY ZONE LABS "AS IS" WITHOUT WARRANTY OF ANY KIND. ZONE LABS DISCLAIMS ANY AND ALL WARRANTIES, WHETHER EXPRESS, IMPLIED, OR STATUTORY, INCLUDING, BUT WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY, AND FITNESS FOR A PARTICULAR PURPOSE. ZONE LABS SHALL NOT BE LIABLE FOR DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, COVER, RELIANCE, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, LOSS OF PROFITS, LOSS OF DATA OR USE, OR BUSINESS INTERRUPTION) ARISING FROM ANY CAUSE ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THE SOFTWARE EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1010
Fls:
3701
Doc:

INDEX

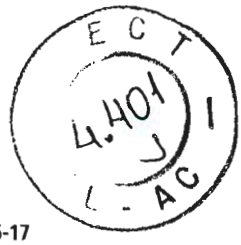
Numerics

802.11x networks
  wireless LANs **4-16**

A

accessing local LAN **3-18**
adapter card for network **2-2**
adding
  backup servers **3-23**
  connection entry **3-5**
address
  remote server
    changing **3-26**
  VPN device **3-7**
Administrator privileges **2-1**
AES algorithm **1-5**
algorithms
  AES **1-5**
  authentication **1-5**
  DES **1-5**
  encryption **1-5**
  HMAC **1-5**
  MD5 **1-5**
  SHA-1 **1-5**
  triple-DES **1-5**
Application Launcher **5-11**
Are You There see AYT firewall policy
authentication
  algorithms **1-5**
  certificate **2-2, 3-8**
  Entrust **3-10**
  features in VPN Client **1-4**
  information
    connection status **4-25**
  internal server **1-4, 4-5**
  methods **1-4, 4-5**
  NT Domain **1-4**
    dialog box **4-6**
    domain name **4-7**
    password **4-7**
    username **4-7**
  properties
    changing **3-20**
  RADIUS **4-5**
  RSA
    next cardcode **4-11**
    passcode **4-8**
    PIN **4-9**
    username **4-8, 4-9**
  SDI
    seeRSA
  SecurID **1-4, 4-8**
  smart card **4-14**
  SoftID **1-4, 4-8**
auto initiation
  authenticating **4-18**
  changing option values **4-20**
  connection failures **4-22**
  connection profile **4-17**
  disabling **4-20, 5-17**
  disabling while suspended **4-21**
  disconnecting **4-19**
  enabling **4-21, 5-17**
  managing **5-16**

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1011
Fls:
Doc: 3701



restarting 4-21
resuming 4-19
retry interval 5-17
states 4-23
suspending 4-19
system tray icons 4-23
using 4-16
Automatic VPN Initiation option 5-16
AYT firewall policy 4-25, 4-28

B

backup servers
adding 3-23
disabling 3-24
enabling 3-23
removing 3-24
Baltimore Technologies 4-11
base 64 encoded file type 6-12
binary encoded file type 6-12
bytes in
connection statistics 4-26
bytes out
connection statistics 4-26

C

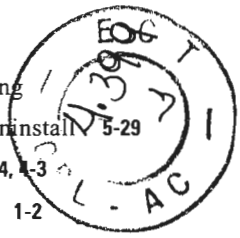
cable
connection 1-2
modem 1-2, 4-2
CA certificates 6-5
Centralized Protection Policy see CPP firewall policy
certificate
changing 3-22
changing password 6-22
completing enrollment form 6-4
connecting 4-11
deleting 6-21
enrollment
file types 6-12
PKI 4-11
with CA 6-4
Entrust 3-10
expiring 4-12
exporting 6-23
importing 6-15
managing 6-17
name 3-5, 3-8, 4-1
stores 6-3
verifying 3-10, 6-20
viewing 6-18
Certificate Authorities (CA)
CA certificates tab 6-5
certificate 2-2
supported 4-11
Certificate Manager
Options menu 6-17
overview 6-1
starting 6-2
changing
certificate 3-22
certificate password 6-22
connection entry description 3-17
connection entry properties 3-14
group name or group password 3-21
password on an enrollment request 6-28
remote server address 3-26
Cisco certificate store 6-3
classes that generate events 5-22
clearing events display 5-24
Client/Server policy
firewalls 4-25, 4-27, 4-31
Client IP address in connection status 4-24
cloning a connection entry 5-3
closing the VPN Client 4-32
common name in certificate enrollment 6-4
company in certificate enrollment 6-4

completing an enrollment request 6-29
compression algorithm
LZS compression 4-25
configuring connections automatically 5-5
connecting
before logon 5-14
to private network 4-2, 4-4
to the internet
via Dial-Up Networking 3-24
to the internet via Dial-Up Networking 4-3
with certificate 4-1
nection
LAN 1-2
network
direct 2-2
properties
changing 3-23
statistics
bytes in 4-26
bytes out 4-26
packets bypassed 4-26
packets decrypted 4-26
packets discarded 4-26
packets encrypted 4-26
resetting 4-32
status
key icon 4-27
local LAN routes list 4-27
secure associations 4-27
secured routes 4-27
time connected 4-27
transparent tunneling 4-25
viewing 4-24
technologies 1-2
connection entry
changing
remote server address 3-26
changing description 3-17
changing properties 3-14
cloning 5-3
creating 3-5
creating shortcut 5-10
definition 3-1
deleting 5-4
description 3-17
managing 5-2
optional parameters 3-14
parameters 3-1
preconfigured 3-1
profile 3-5
properties
changing 3-14
renaming 5-5
copyrights and licenses A-1
country code in certificate enrollment 6-5
CPP firewall policy 4-25, 4-29
creating
connection entry 3-5
shortcut for connection entry 5-10

D

data
formats xii
Data Encryption Standard
see DES algorithm
Dead Peer Detection
see DPD
deleting
certificate 6-21
connection entry 5-4
enrollment request 6-27
department in certificate enrollment 6-4
DES algorithm 1-5
DHCP request 1-3
DHCP traffic
stateful firewall always on 5-11

ECT 4.400 J CPL - AC
ROS Nº 03/2005 - CN CPMI - CORREIOS 1012 Fls: Doc:



Dial-Up Networking
  closing before uninstall 5-29
  connecting 3-24, 4-3
  dial-up modem 1-2
  disabling 3-25
  enabling 3-25
  icon on taskbar 4-4
  Microsoft 1-3
  phonebook entries 3-25
  programs
    third party 3-26
    uirement for 2-2
  User Information dialog box 4-3
Digital Subscriber Line
  see DSL
direct network connection 2-2
disabling
  application launch before startup 5-15
  automatic disconnect when logging off Windows NT 5-16
  backup servers 3-24
  Dial-Up Networking 3-25
  local LAN access 3-18
  Logon to Microsoft Network parameter 3-20
  third party dial-up 3-26
disconnecting
  automatic 5-16
  private network 4-32
Disk icon in log viewer 5-24
displaying
  help 3-1
  software version 3-3
DNS
  dynamic 1-3
  split 1-4
documentation
  cautions xii
  notes xii
domain
  Certificate Authority 6-7
  name
    certificate enrollment 6-5
    NT Domain authentication 4-7
  server 1-4
DPD
  adjusting peer time out 3-19
  keep alive mechanism
DSL
  connection technology 1-2
  modem 1-2, 4-2
DUN phonebook entries 3-26

E

e-mail address in certificate enrollment 6-5
enabling
  auto initiation 5-17
  backup servers 3-23
  local LAN access 3-18
  logging on to Microsoft Network 3-20
  start before logon 5-14
  stateful firewall 5-11
  transparent tunneling 3-17
encryption
  algorithms 1-5
  connection status 4-25
enrolling
  certificates 6-4
    file request 6-11
    network 6-6
  in a PKI 4-11
enrollment request
  changing password 6-28
  completing 6-29
  deleting 6-27
  form 6-4
  managing 6-25

pasting **6-11**
resuming **6-29**
viewing **6-26**
Entrust
certificate
configuring **3-10**
connecting with **4-12**
SignOn
using with start before logon **4-14**
Technologies **4-11**
Erase icon in log viewer **5-24**
ase User Password option **4-6, 5-7**
ESP
protocol
transparent tunneling **3-17**
traffic
stateful firewall always on **5-11**
etoken
connecting with **4-14**
events
classes **5-22**
collecting **5-19**
severity levels **5-21**
viewing and managing **5-17**
exiting the VPN Client **4-32**
exporting a certificate **6-23**

F

F1 key
displaying help **3-1**
features of VPN Client **1-3**
file types for certificate enrollment **6-12**
Filter icon in log viewer **5-20**
filtering
events **5-20**
firewalls **4-29**
firewalls **4-30**
AYT tab **4-28**
Client/Server policy **4-25, 4-27, 4-31**
CPP firewall policy **4-29**
filtering **4-29**
ICMP protocol **4-30**
matching **5-26**
name on general status
notifications **5-26**
policies **4-25**
policy listed **4-25**
rules **4-29**
stateful **5-11**
status **4-27**
status screen **4-25**
support in VPN Client **1-5**
tab on status screen **4-25**
TCP protocol **4-30**
UDP protocol **4-30**
force keepalives
ESP-aware NAT **3-18**
formats
data **xii**

G

General tab (Properties) **3-17**
generating events
classes **5-22**
group name for IPSec
changing **3-21**
group password for IPSec
changing **3-21**

H

hard disk space requirement **2-2**
Hashed Message Authentication Coding
see HMAC algorithm

ECT 4.398 J CPL - AC
RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1013
Doc: 3701

help
displaying 3-1
F1 key 3-1
from program menu 3-1
Help icon in log viewer 5-19
HMAC algorithm 1-5
hostname
VPN device 3-7

I

I/O protocol numbers 4-30
ICMP protocol
firewalls 4-30
icons
Dial-Up Networking 4-4
key 4-27
log viewer
Disk 5-24
Erase 5-24
Filter 5-20
Help 5-19
Printer 5-23
Search 5-22
VPN Client
viewing connection status 4-24
viewing when connected 4-16
VPN Dialer
using to disconnect 4-32
IKE Keepalives 1-4
IKE protocol 1-2
importing
certificate file 6-15
configuration 5-5
Import Password 6-16
inactivity timeout (Entrust) 4-12
installing
media requirements 2-2
installing VPN Client
InstallShield 2-3
MSI 2-5
process 2-1
interface card for network 2-2
internal server
authentication 1-4, 4-5, 4-6
internet
connecting via Dial-Up Networking 3-24, 4-3
Internet Key Management protocol
see IKE
Internet Protocol Security
see IPSec
IOS
platform devices supported x
IP address
certificate enrollment 6-5
server 4-24
VPN device 3-7
IPSec
attributes supported in VPN Client 1-5
features in VPN Client 1-4
group name 3-21
group password 3-21
over TCP 3-18
over UDP 3-18
protocol 1-2
transparent tunneling
connection status 4-25
ISDN
connection technology 1-2
modem 4-2
ISP
password 4-3
username 4-3

E C
1 4.396 1
CPL - AC

K

key icon
  connection status 4-27

L

LAN connection 1-2
launching an application 5-11, 5-15
licenses and copyrights A-1
local LAN access 3-18
  connection status 4-27
log file
  printing 5-23
  saving 5-24
logging on to Microsoft Network 3-20
log viewer
  clearing 5-24
  filtering events 5-20
  icons
    Disk 5-24
    Erase 5-24
    Filter 5-20
    Help 5-19
    Printer 5-23
    Search 5-22
  options
    capture 5-19
    filter 5-20
  searching 5-22
LZS compression 4-25

M

maintenance dialog
  MSI 2-8
managing
  auto initiation 5-16
  certificates 6-1, 6-17
  connection entries 5-2
  enrollment request 6-25
  event log 5-17
matching firewall configurations 5-26
Message Digest 5 (MD5) algorithm 1-5
Microsoft
  Certificate Services 4-11
  certificate store 6-3
  Network
    logging on 3-20
  Windows 2000 4-11
  Windows Installer (MSI)
    installing VPN Client 2-5
modems
  cable 1-2, 4-2
  dial-up 1-2
  DSL 1-2, 4-2
  ISDN 4-2
  requirement 2-2
MSI 2-5
  installation 2-5
    removing 5-32
  maintenance dialog 2-8
  repair dialog 2-8

N

names
  IPSec group 3-21
NAT 3-17
network
  adapter or interface card 2-2
  connection
    direct 2-2
Network Address Translation 3-17
New Connection Entry Wizard 3-6
notifications
  firewall 5-26
  upgrade 5-25

ROS Nº 03/2005 - CN
CPMI - CORREIOS
1014
Fls:
Doc: 3701

VPN device 5-25
NT Domain authentication 1-4, 4-6
domain name 4-7
password 4-7
username 4-7
NT features
logon 5-14
VPN Client 1-3

O

options
Application Launcher 5-11
auto disconnect 5-16
Automatic VPN Initiation 5-16
Clone entry 5-3
Delete entry 5-4
Erase User Password 5-7
Import entry 5-5
Rename entry 5-5
Save Password 5-7
shortcut 5-10
start before logon 5-14
Stateful Firewall (Always on) 5-11
Windows
Logon Properties 5-14
Options menu 3-14
organizational unit in certificate enrollment 6-4
organization of this manual ix

P

packets
bypassed 4-26
decrypted 4-26
discarded 4-26
encrypted 4-26
parameters
connection entry 3-1
passcode
RSA authentication 4-8
passwords
enrollment request
changing 6-28
erasing 4-6, 5-7
expiration 4-7
import 6-16
internal server authentication 4-6
invalid 4-6
IPSec group
changing 3-21
ISP logon 4-3
NT Domain authentication 4-7
personal certificate 6-22
private key 4-1
RADIUS authentication 4-6
saving 4-6, 5-7
PAT 3-17
Peer Certificate Domain Name Verification 1-4
peer response timeout
adjusting 3-19
personal firewall see firewalls
phonebook entries
DUN 3-26
PIN
RSA authentication 4-9
PKCS10 format 6-12
PKIs
supported 2-2, 4-11
Plain Old Telephone Service
see POTS
port
transparent tunneling 4-25
Port Address Translation 3-17
POTS
connection technology 1-2

preconfigured connection entry 3-1
Printer icon in log viewer 5-23
printing a log file 5-23
private key password 4-1
private network
  connecting 4-2, 4-4
  disconnecting 4-32
privileges required for
  installing VPN Client 2-1
profile
  connection entry 3-5
  Entrust 3-11
  file
    importing into VPN Client 5-5
  roaming 5-16
properties
  general 3-17
Properties dialog box 3-15
Protocol 50 (ESP) traffic 3-17
protocol numbers 4-30
protocols
  DPD
  ESP 3-17
  ICMP 4-30
  IKE 1-2
  IPSec 1-2, 3-18
  TCP 3-17, 4-30
  UDP 3-17, 4-30
Public Key Infrastructure
  see PKIs

Q

quitting the VPN Client 4-32

R

RADIUS authentication
  password 4-6
  procedure 4-5
  username 4-6
RAM requirements 2-2
reconfiguring automatically 5-5
remote access connection
  closing before uninstall 5-29
Remote Authentication Dial-In User Service
  see RADIUS authentication
remote server
  changing address 3-26
removing
  backup servers 3-24
  the VPN Client
    InstallShield 5-29
removing a client configuration
  the VPN Client
    MSI 5-32
renaming a connection entry 5-5
repair dialog
  MSI 2-8
requirements
  system 2-1
resetting connection statistics 4-32
restarting your computer after installation 2-4
resuming an enrollment request 6-29
retry interval
  auto initiation 5-17
roaming profiles 5-16
RSA (formerly SDI)
  authentication 1-4, 4-8
  Next Cardcode 4-11
  passcode 4-8
  PIN 4-9
rules
  firewalls 4-29

ECT 14.394 SOL - MS
RQS Nº 03/2005 - CN
CPMI - CORREIOS
1015
Fls:
3701
Doc:

S

Save Password option **4-6, 5-7**
saving a log file **5-24**
SCEP (Cisco store) **6-3**
SDI
  see RSA
Search icon in log viewer **5-22**
searching log file **5-22**
secure associations **4-27**
secured routes
  connection status **4-27**
  icon **4-27**
secure gateway
  address **3-7**
  notifications to client **5-25**
Secure Hash Algorithm
  see SHA-1 algorithm
SecurID authentication **1-4, 4-8**
Server IP address
  connection status **4-24**
setting or changing connection entry properties **3-14**
Severity levels in events **5-21**
SHA-1 algorithm **1-5**
shortcut
  creating for connection entry **5-10**
Simple Certificate Enrollment Protocol
  see SCEP
smart card
  connecting with **4-14**
  connection entry
    configuring **3-11**
  products supported **3-12**
SoftID authentication **1-4, 4-8**
software license agreement **A-1**
software token applications
  launching from VPN Dialer **5-11**
split DNS **1-4**
split tunneling **1-4**
start before logon
  configuring **5-14**
  using with Entrust SignOn **4-14**
starting the VPN Dialer
  connecting to private network **3-5, 4-2**
  using a shortcut **5-10**
stateful firewall
  always on **5-11**
  DHCP traffic **5-11**
  transparent tunneling **3-17**
state in certificate enrollment **6-4**
statistics
  connection time **4-27**
  local LAN routes **4-27**
  packet **4-26**
  secured routes **4-27**
status
  firewall **4-27**
stopping the VPN Dialer **4-32**
stores
  certificate **6-3**
system requirements **2-1**

T

TCP/IP requirement **2-2**
TCP protocol
  firewalls **4-30**
  transparent tunneling **3-17**
third party dail-up program **3-26**
time connected
  connection status **4-27**
transparent tunneling
  enabling **3-17**
  port **4-25**
  stateful firewall **3-17**
triple-DES algorithm **1-5**

tunnel
definition 1-2
negotiation 4-4
transparent 3-17

U

UDP protocol
firewalls 4-30
transparent tunneling 3-17
UniCERT 4-11
installing the VPN Client
InstallShield 5-29
MSI 5-32
upgrade notification 5-25
upgrading VPN Client software
using InstallShield 5-27
using MSI 5-29
URL or Network Address of CA 6-7
user authentication 1-4, 4-5
see also authentication
username
internal server authentication 4-6
ISP logon 4-3
NT Domain authentication 4-7
RADIUS authentication 4-6
RSA authentication 4-8, 4-9

V

verifying a certificate 3-10, 6-20
version
VPN Client
displaying 3-3
viewing
certificate 6-18
connection status 4-24
enrollment request 6-26
Virtual Private Network (VPN)
defined 1-1
VPN
defined 1-1
VPN Client
applications 1-1
event log 5-17
features 1-3
installing 2-1
software updates 5-27, 5-29
version 3-3
VPN Client version 3.6
removing 2-8
VPN Concentrator
see VPN device
VPN device
authentication using internal server 4-5
backup 3-23
changing address 3-26
Cisco 1-1
DPD 3-19
hostname 3-7
IP address 3-7
notifications 5-25
VPN Dialer
closing 4-32
main dialog box 3-6

W

Windows
NT logon properties 5-14
platforms requirement 2-1
username and password 3-20
wizard
connection entry 3-6
WLANs
auto initiation 4-16

4.3921
RQS Nº 03/2005 - CN
CPMI - CORREIOS
1016
Fls:
Doc: 3791

X

X.509 DER file **6-12**

Z

Zone Labs Integrity **4-25, 4-27, 4-31**

Apendice CF

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1017
Doc: 3701

Cisco Confidential

Table of Contents

Q & A
Cisco 1751 Modular Access Router

Product Features and Positioning
Software Feature Sets
LAN Functionality
WAN Functionality
Voice Functionality
Cisco IOS Security
Processor
Performance
Internal Expansion Slot and Encryption Card
Compression
IBM/SNA Features
Memory Architecture
Power Supply
MTBF
Network Management

Q & A

Cisco 1751 Modular Access Router

Product Features and Positioning

Q. 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

ECT 1 4.389 1 CPL - AC

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

RQS Nº 03/2005 - CN CPMI - CORREIOS 1019 Doc: 3791

ECT 1 4.388 1 CAL - AC

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

ROS Nº 03/2005 - CN
CPMI - CORREIOS
1020
Fls: 3701
Doc:

We urge the customers to migrate to the Cisco 1751 due to the clear advantages that it offers at the same price oint. The Cisco 1751 Router provides all of the features of the 1750 plus support for; digital voice, VLAN, and reater performance. In addition, the Cisco 1751 Router comes with more memory than the 1750 (both flash nd DRAM), which reduces the overall solution cost when deploying voice and/or security features.

). What are the differences between the Cisco 1600-R series and the Cisco 1700 series router?

. Compared with the Cisco 1600-R series, the Cisco 1700 series offers increased performance, added lexibility with fully modular chasses, and investment protection with support for new services such as DSL, oice over IP (VoIP), and VPNs at similar price points to the Cisco 1600-R. Wherever possible, Cisco ncourages customers to move to the new Cisco 1700 platform to be best positioned for future growth and ervices. Some services (DSL, VoIP) are and will not be supported on the Cisco 1600-R series because of erformance and architecture limitations. Table 3 clarifies the features of the Cisco 1600-R and 1700 series amilies. The Cisco 1600-R series will continue to be available, but Cisco is actively marketing the 1700 series s 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 s $1595 (US list). For $100, customers get the added benefits of increased performance and the ability to enefit 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	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

RQS Nº 03/2005 - CN - CPMI - CORREIOS
1021
Fls: 3701
Doc:

	Single serial with integrated T1/FT1 DSU: WIC-1DSU-T1	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)

ECT 1 4.386 1 J CPL - AC

ROS Nº 03/2005 - CN - CPMI - CORREIOS 1022 Fls: Doc: 3701

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 Card	No	Yes
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

RQS Nº 05/2005 - CN
CPMI - CORREIOS
1023
Fls.
Doc: 3701

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 or 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

). When would a customer want a Cisco 2600 series router rather than a Cisco 1751 router?

. The Cisco 2600 series is better suited for larger enterprise branch offices that require multiple WAN ports nd, typically, a 19-inch rack-mount enclosure. It provides two WAN interface card slots, plus an additional etwork module slot, which provides higher port densities as well as support for voice services. The key ifferences are highlighted in Table 4.

'ab): 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

ECT 1.350 DPL - AC
ROS Nº 03/2005 - CN
CPMI - CORREIOS
1024
Fls:
3701

	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

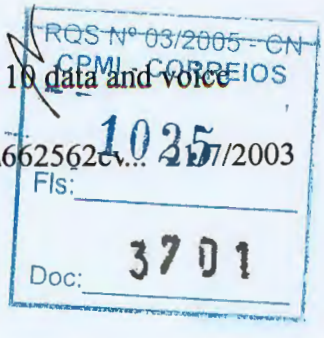
Q. Which Cisco IOS® release is available with the Cisco 1751 at first customer ship (FCS)?

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



nages.

able 5: Minimum Memory Requirements and Software Feature Sets for Cisco OS 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

ECT 4.382 CPL - A
RQS Nº 03/2005 - CN - CPMI - CORREIOS
1026
Fls:
Doc: 3791

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

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1027
Fls:
Doc: 3701

	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

ECT 1 1380 CPL - AC

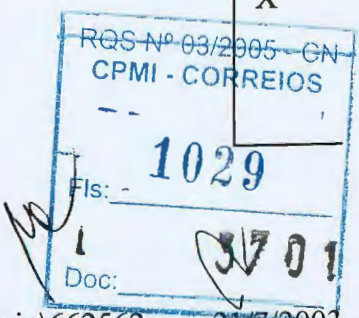
RQS Nº 03/2005 - CN CPMI - CORREIOS 1028 Fls 3701

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/AD FW/I
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

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1030
Doc: 3701

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/A Plus 3DE
WAN	Frame Relay SVC	X	X	X	X
IP Routing	BGP	X	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

RQS Nº 03/2003 - CN
CPMI - CORREIOS
1031
Fls:
Doc: 3701

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	X	X	X	X

ECT 1 4.376 1 CPL - AC

RQS Nº 03/2005 - CN CPMI - CORREIOS 1032 Fls: 3701 Doc:

	generation				
	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

AN Functionality

). What types of LANs does the Cisco 1751 router support?

. 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 r directly to a PC Ethernet port (using a crossover cable) using inexpensive, unshielded twisted-pair (UTP) iring.

). Is the 10BaseT Ethernet WIC supported on the 1751?

. Yes, the 10Base T Ethernet WIC is supported on the 1751 to provide dual Ethernet functionality.

). What LAN and routing protocols are supported by the Cisco 1751 router?

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1033
Fls:
Doc: 3701

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 autonegotiated.

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).

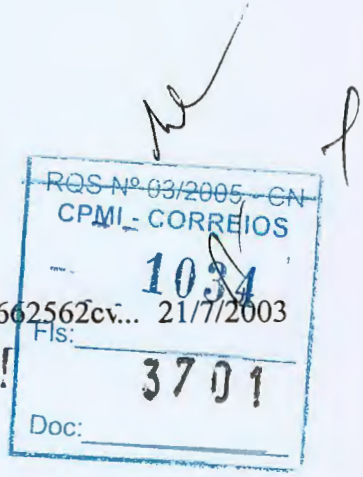
WAN Functionality

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

. Are there any WIC slot dependencies with respect to order or maximum number of a certain type?

. All WICs are supported in any slot and in any combination.

. Does the Cisco 1751 router support two ISDN BRI interfaces?

. Yes. The Cisco 1751 router supports two BRI interfaces (dial and ISDN leased line) with two ISDN BRI 'AN interface cards installed in the two WAN interface card slots. Multilink PPP (MP) can combine the four channels to achieve data rates up to 256 Kbps.

. Do the WIC-1T, WIC-2T, and WIC-2A/S WAN interface cards support asynchronous serial when installed the Cisco 1751 router?

. Y The Cisco 1751 router supports asynchronous serial (up to 115.2 Kbps) as well as synchronous serial or e ial WAN interface cards. The onboard aux port also supports asynchronous serial at speeds up to 115.2 bps.

. What WAN protocols does the Cisco 1751 router support?

. Point-to-Point Protocol (PPP), High-Level Data Link Control (HDLC), X.25 Link Access Procedure, alanced (LAPB), Switched Multimegabit Data Service (SMDS), Frame Relay, and IBM/SNA are supported ver permanent or switched digital lines. PPP and Serial Line Internet Protocol (SLIP) are supported over synchronous analog lines.

. Do the serial ports on the Cisco 1751 router support data-communications-equipment (DCE) functionality?

. Yes, the Cisco 1751 router supports DCE (that is, supplies clocking), allowing the Cisco 1751 router to terconnect without requiring a null modem. Also, X.25 packet assembler/disassembler (PAD) functionality is pported. IBM Synchronous Data Link Control (SDLC), bisync, and other serial protocols are supported.

. DSL supported on the Cisco 1751?

. No.

. Will the Cisco 1751 support three WICs?

. The Cisco 1751 can only support two WAN interfaces. The AUX port can be used as another WAN port. If our customer needs greater density, the Cisco 2600 would be the solution.

. Does the Cisco 1751 Router support Modem WIC card?

. Yes. The Cisco 1751 Router supports one and two-port V.90 modem WIC card. Product number is WIC-AM and WIC-2AM. For more details about the Modem WIC, please refer to the following data sheet:

ttp://www.cisco.com/warp/public/cc/pd/rt/1700/prodlit/17srt_ds.htm

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1035
Fls:
Doc: 3701

'oice Functionality

. Does Cisco 1751 support Survivable Remote Site Telephony (SRST)?

. Yes. For the detailed information, please refer to the below documents

nnouncement: http://www.cisco.com/cpropart/salestools/cc/pd/rt/1700/prodlit/1601_po.htm

atasheet: http://www.cisco.com/warp/partner/synchronicd/cc/pd/unco/srstl/prodlit/srstd_ds.htm

. What voice interface cards (VICs) are supported on the Cisco 1751?

. The voice interface cards currently supported are given in Table 10.

able 10: Voice Interface Cards Currently Supported

Voice Interface Card	Interfaces
V 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

RQS Nº 03/2005 - CN - CPMI - CORREIOS
1036
Fls.
Doc: 3701

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

E
Fl. 3711
CPL - AC

. How many DSPs are supported in the 1751?

. The 1751 has 2 DSP module slots on the motherboard, each of which supports the 5 DSP module. This ovides a DSP density of 10 DPS's.

. What are the PVDM/VIC combinations that are supported?

. The supported combinations are shown in Table 11.

able 11: Supported PVDM/VIC Combinations

PVDM	Number of DSPs Supported	VIC Combinations
PVDM-256K-4	1	1 analog VIC
PVDM-2[illegible]-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

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1032
Fls:
Doc: 3701

		Up to 2 voice-BRI VICs or Upto 2 analog VICs+1 voice- BRIVIC or 1 analog VIC+up to 2 voice-BRI VICs

). Are the PVDM-4 (supported in Cisco 1750) supported in Cisco 1751?

.. PVDM-4, 8,12 are not officially supported in the Cisco1751.

). Are the PVDM-256K-4 (supported in Cisco 1751) supported in Cisco 1750?

.. PVDM-256K-4, 8,12 are not officially supported in the Cisco1751.

). Does the 1751 support digital VICs?

.. Yes, the 1751 supports digital VICs. At FCS, the ISDN BRI NT/TE VIC is supported, and 1 or 2 port T1/E1 'WICs are supported in Cisco IOS 12.2(4)YB or later releases.

). Does the Cisco 1751 support the T1/E1 VWICs (i.e. the multi-flex cards)?

.. Yes. From Cisco IOS 12.2(4) YB or later releases. It will roll into 5th 12.2 T train release.

). How many DSPs are required to support the various VICs?

). The analog VICs require 1 DSP/VIC, the ISDN BRI VIC requires 2 DSPs/VIC. For T1/E1 VWICs, it epends on the codec and how many voice channels are used. The number of maximum channels support per)SP is listed in Table 12.

'able 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.

ECT 21.3701 J CPL-AC

ROS nº 02/0005-CN CPMI - CORREIOS 1038 Fls: 3701 Doc:

SP used for the digital calls and for the analog calls have to be calculated separately and one DSP can support ultiple Codecs concurrently for T1/E1 VWICs.

. Does Cisco 1751 support Caller ID?

. Yes, Cisco 1751 supports Caller ID transmission on FXS, FXO-M1 and FXO-M2 interfaces. It provides aller ID blocking configurable at the source location on FXS, and ability to unblock Caller ID on FXO-M1, I2 interfaces.

. Does Cisco 1751 support analog DID trunk card?

. Yes.

. What does toll reduction or toll bypass mean?

. In most of today's corporate networks, voice networks are separate from data networks. Typically, data etworks are priced by a monthly fixed cost basis and are usually much cheaper than the voice networks. An xample of this is a leased-line environment. In this case, the customer pays for that network, whether data is owing or not. In a typical phone network, charges are incurred on a usage basis. Therefore, phone expenses on iteroffice dialing can be quite expensive, especially since most interoffice calling occurs during "peak" us s hours.

/hen you have the ability to put your interoffice voice calls across a lower-price or fixed-price network with a roduct such as the Cisco 1751 platform, you can avoid the "toll" that is charged by the long-distance carrier, ocal exchange carrier (LEC), or Port, Telephone, and Telegraph (PTT). The voice call then travels over the ime network that your data travels over and avoids going into the Public Switched Telephone Network (PSTN) nd, therefore, does not incur charges.

is easy for companies to figure out the savings that they will get, because they receive accurate monthly eports that describe their costs from their LECs. Any company that does a great deal of interoffice calling will ave more money than one that does more "off-net" PSTN-type calling.

. What do the terms FXO, FXS, and E&M mean?

. The Cisco 1751 router supports FXO, FXS, and E&M voice interface cards. Each type provides a slightly ifferent interface for connecting to different types of equipment.

'or n Exchange Office

'he FXO interface allows an analog connection to be directed at the central office (CO) of the PSTN. This nterface is of value for off-premise extension applications. This is the only voice interface card that will be pproved to connect to off-premise lines. This interface may be used to provide backup over the PSTN or for 'entrex-type operations. This voice interface card needs to be approved by PTTs; it is not available in every ountry. Check the homologation status page at http://wwwin-ng.cisco.com/Eng/MSABU/Eng_Ops/WWW/index.htmfor up-to-date availability information.

'oreign Exchange Station

'he FXS interface allows connection for basic telephone service phones (home phones), fax machines, keysets, nd private branch exchange (PBXs) by providing ring voltage, dial tone, and so on. This interface will be used /here phones are connecting directly to the router. FXS will be very popular for trials because it allows the hones to be plugged directly into the router.

ECT 4.3691 J

CPMI - CORREIOS 1039 Fls: 3701 Doc:

ar and Mouth

he 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.

. What's the difference between FXO and FXO-M1, FXO-M2?

. VIC-2FXO-M1 and VIC-2FXO-M2 support battery reversal detection and Caller ID. While the regular VIC-FXO doesn't. VIC-2FXO-M1 is for U.S. and Canada, VIC-2FXO-M2 is for Europe.

. Does the Cisco 1751 support three analog VICs, or six analog voice ports?

. Yes. Customers requiring this capability need to order the PVDM-256k-12 module (part number: PVDM-56k-12=), which provides three DSPs.

. Is RAS for H.323 gatekeeper registration supported on the Cisco 1751 platform?

. Yes.

. In 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 isco 1751?

. The FXS port does not have the ability to provide the voltage levels necessary to perform this function.

. What are the key features when implementing voice on the Cisco 1751?

. Please refer to Cisco 1700 Modular Access Voice Feature Overview

ttp://wwwin.cisco.com/cmc/cc/pd/rt/1700/sales/orwir_st.htm

Cisco IOS Security

. What security functions are available for the Cisco 1751 router?

. 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.

. Can I use the Cisco 1751 router as a firewall?

. 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: ttp://www.cisco.com/warp/partner/synchronicd/cc/cisco/mkt/security/iosfw/index.htmpartner/synchronicd/cc/ci

. Can I encrypt data on the Cisco 1751 router?

CPMI - CORREIOS
1040
Fls:
Doc: 370

. Yes. Two types of encryption technologies are supported: IPSec Data Encryption Standard (DES) 56 and 'Sec Triple DES.

'rocessor

. What is the processor on the Cisco 1751 router?

. The Cisco 1751 router uses a Motorola MPC860P PowerQUICC at 48 MHz. The Cisco 2600 series uses an PC860. The 860P processor of the Cisco 1751 router has an integrated Fast Ethernet controller. This has ıplications on performance, as discussed in the Performance section.

'erformance

. How does the performance of the Cisco 1700 series compare to that of the Cisco 1600-R series?

. As Table 13 shows, the Cisco 1751 router performance is greater than that of the Cisco 1600-R series.

able 13: Performance Comparison of the Cisco 1600-R Series and the Cisco 1751

F ıre	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)

. How does the performance of the Cisco 1751 router compare with that of the Cisco 2600 series routers?

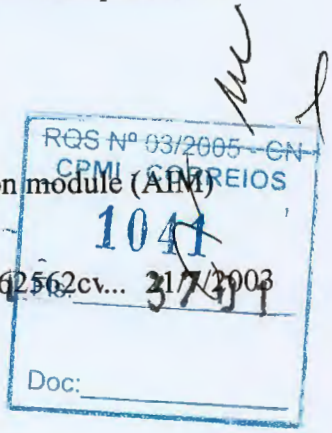
. The Cisco 2600 series router has higher fast-switching performance (12,000 to 37,000 pps for 64-byte ıckets) compared to the Cisco 1751 router (8400 pps). However, the encryption and process switching erformance for both platforms are similar (512 Kbps for IPSec DES 56 encryption with 256 byte packets; 768 bp r 1500 pps for process switching of 64-byte packets).

. Why is the fast-switching performance of the Cisco 1751 router not equal to that of the Cisco 2600 series hen they appear to use the same processor?

. The Cisco 1751 router uses a Motorola MPC860P processor, which is different from the MPC860 processor ı the Cisco 2600 series. The Motorola 860P has an integrated Fast Ethernet controller. This processor uses an bitration scheme that continuously polls for contenders for the Fast Ethernet bus in a round-robin fashion. ontenders are the serial communications controllers (SCCs), Ethernet controller, and cache. This process of ound-robin polling uses up clock cycles, resulting in lower fast-switching performance.

nternal Expansion Slot and Encryption Card

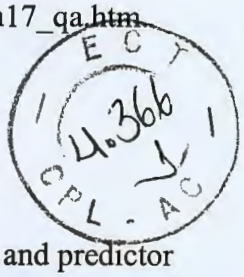
. Can the internal expansion slot of the Cisco 1751 router support the advanced integration module (AIM) xpansion cards (for example, encryption) that is supported on the Cisco 2600 series?



. No. The Cisco 2600 series has an AIM slot that is based on a protocol control information (PCI)-bus chitecture; the Cisco 1751 router, on the other hand, uses a Q-bus to lower cost. Although the expansion cards ı these platforms are not the same, the encryption technology is interoperable and, therefore, creates a ɔmplete Cisco end-to-end solution.

. Does the Cisco 1751 support the 1700 VPN module that accelerates DES and 3DES for IPSec?

. Yes. See VPN Module Q&A at:
tp://wwwin.cisco.com/Mkt/cmc/cc/cisco/mkt/access/1700/internal/vpn17_qa.htmvpn17_qa.htm



ɔmpression

. Does the Cisco 1751 router support compression?

. Yes. Up to 4:1 compression is supported. The Cisco 1751 router supports both Stac and predictor ɔmpression algorithms. Compression performance for the Cisco 1751 router has not been measured yet.

. What compression algorithms are supported on the Cisco 1751 router?

. T WAN interfaces of the Cisco 1751 router support the types of compression algorithms for each of the 'AN encapsulations given in Table 14.

able 14: Compression Algorithms
ıpported on the Cisco 1751 Router

Encapsulation	Compression Algorithm
PPP	Predictor stacker
Frame Relay	Payload
HDLC	Stac
X.25	Payload
L B	Predictor Stac

BM/SNA Features

). What IBM/SNA features are available for Cisco 1751 router?

.. The supported IBM/SNA features on the Cisco 1751 router are equivalent to those supported on the Cisco 600-R, 2500, and 2600 series routers (see Table 15):

'able 15: IBM/SNA Features Supported on the Cisco 1751 Router

STUN	NetBIOS

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1042
Fls: 3701
Doc:

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

ot Token Ring and Advanced Peer-to-Peer Networking (APPN), supported on the Cisco 2500 and 2600 eries, are not supported on Cisco 1600-R series and 1751 routers.

). Will the Cisco 1751 router support Token Ring interfaces?

.. No, there are no plans to support Token Ring on the Cisco 1751 router.

). When do I sell a Cisco 1751 router IBM solution?

.. 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

). What IBM/SNA software feature sets are available for Cisco 1751 router?

.. 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

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1043
Fls:
Doc: 3701

- IP/ADSL/IPX/AT/IBM/FW/IDS/Voice Plus IPSec 3DES

---

ote Use Plus for L2F, L2TP, BGP, NTP, NLSP, RSVP, IP multicast, Frame Relay SVC, and encryption ıpport.

Iemory Architecture

. What memory architecture does the Cisco 1751 router use?

. The Cisco 1751 router uses the run-from-RAM memory architecture.

. What type of DRAM memory does the Cisco 1751 router use?

. The Cisco 1751 router uses synchronous DRAM (SDRAM). The default DRAM is 32 MB fixed onboard for e 1751 model, and 64 MB for the 1751-V model. There is one DIMM slot for adding additional memory in crements of 16, 32, and 64 MB. The maximum DRAM for the 1751 model is 96MB (32 MB onboard plus 64 B 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

. What type of Flash memory does the Cisco 1751 router use?

. The Cisco 1751 router uses onboard (soldered on the motherboard) flash. The Cisco1751 has 16 MB of ash. The Cisco 1751-V have 32 MB of flash. This is a fixed configuration—it is not upgradeable and there is ot a flash card slot on the motherboard to add more flash.

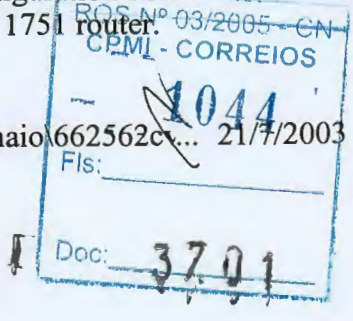
	Cisco 1751	Cisco 1751-V
I ult Flash (MB)	16	32
Max. Flash (MB)	16	32

. What is the flash memory used for?

.. Cisco IOS software and configuration files are stored flash. Also, flash memory allows software upgrades to e downloaded over the WAN or LAN link to be stored in the Mini-Flash card.

. How are software images and configuration files stored in flash?

.. Flash come preprogrammed with Cisco IOS software. Software upgrades and configuration files must be opied using Trivial File Transfer Protocol (TFTP) onto a Mini-Flash card in a Cisco 1751 router.



). Is dual Flash bank supported on Cisco 1751 routers?

. Yes. Dual Flash bank is supported. Although both the Cisco 1751 and Cisco 1751-V support dual flash bank, e recommend that customers requiring dual flash bank purchase the Cisco 1751-V model since it comes with 2 MB flash.

). Does the Cisco 1751 use the same DRAM as the Cisco 1720/1750?

. Yes. However, the Cisco 1751 does not support the 4 and 8 MB DIMM (MEM1700-4D= and MEM1700-D=). In addition there is a new 64MB DIMM available for the Cisco 1751

). Does the Cisco 1751 use the same flash as the Cisco 1720/1750?

. No. The flash in the Cisco 1751 is soldered on the motherboard, and is therefore not upgradeable.

). Can the amount of shared (input/output [I/O]) memory on a Cisco 1751 router be configured?

. Yes. It can be modified using Cisco IOS command-line interface (CLI) and saved as part of the router onfiguration.

'ower Supply

). What type of power supplies does the Cisco 1751 router use?

. The Cisco 1751 router uses one universal power supply that is applicable for all countries. There are no ountry- specific power supplies. The AC input voltage of this universal power supply spans from 100 to 240 ; the frequency from 47 to 64 Hz. (Although this power supply works in all countries, the user still has to ecify the power cord appropriate for a particular country.) The router also has a locking connector on the ower socket to ensure that the power cord remains securely fastened.

ITBF

). What is the mean time between failures (MTBF) for the Cisco 1751 router?

. The predicted MTBF is 514,526 hours. This predicted MTBF includes the chassis and external power supply ut not the WAN interface cards or voice interface cards.

Network Management

). How is the Cisco 1751 router managed?

. 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 oftware.

). Do CiscoView, CiscoWorks2000, and Cisco Voice Manager support Cisco 1751 routers?

. Yes, CiscoView, CiscoWorks2000 and Cisco Voice Manager supported.

). Does Cisco ConfigMaker support Cisco 1751 routers?

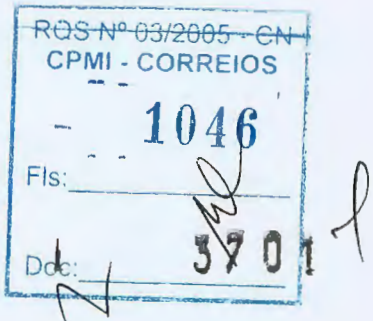
RQS Nº 03/2005 - CN - CPMI - CORREIOS
1045
Fls:
3701
Doc:

A. Yes, Cisco ConfigMaker supports Cisco 1751 routers, starting with Release 2.5b.

Q. Does the Cisco 1751 router support Remote Monitoring (RMON)?

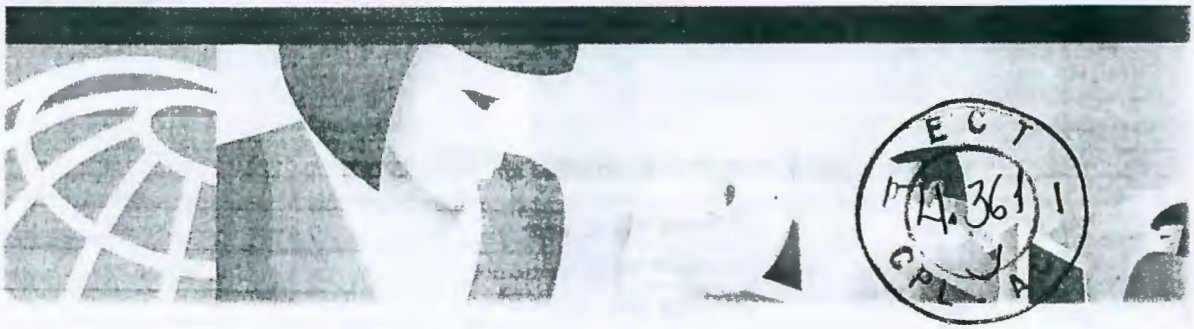
A. The Cisco 1751 router supports only RMON lite. RMON lite covers two out of the nine RMON groups, alarms, and events. Full RMON (statistics, history, hosts, hostTopN, matrix, filter, capture) features are available for the Cisco 2500 and 2600 series routers.

Posted: Wed Aug 21 23:43:46 PDT 2002
All contents are Copyright © 1992--2002 Cisco Systems, Inc. All rights reserved.
Important Notices and Privacy Statement.



Apêndice CG

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1047
Doc: 3701



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.

ROS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1048
Doc: 3701

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.

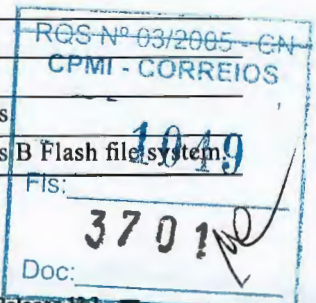
Examples

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 the 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.

ECT copy 4.355 CAL - AC

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.

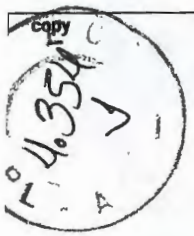
The entire copying process may take several minutes and differs from protocol to protocol and from network to network.

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

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1051
Fls:
Doc 3701



- 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.

ECT 4.353 1 CPLA

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.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1052
3701

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.

ECT 4.351 J AC

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.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1053
Fls:
3701
Doc:

- 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... eeee
```

```
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... eeeeeeeeeeeeeeeeeeeeeeeeeeeeeee ...erased
Connected to 172.23.1.129
Loading 1711088 byte file c3600-i-mz:
!!!
```

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.

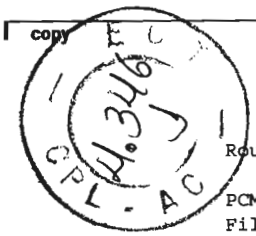
The system will prompt if there are two or more partitions. If the partition entered is not valid, the process terminates. You have the option to enter a partition number, a question mark (?) for a directory display of all partitions, or a question mark and a number (?*number*) for a directory display 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.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1055
Fls:
3701
Doc:



```
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
!!!
```

```
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... eeee
```

ECT 1 4.343 1 J CPL - AC
Copy

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:

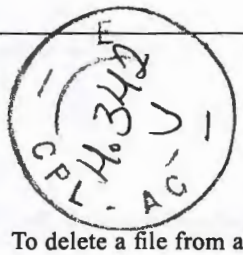
```
copy slot1:router-image slaveslot0:
```

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.

RQS Nº 03/2005 - CN - CPMI - CORREIOS
1057
Fls:
3701
Doc:

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.

ECT
4.341
CPL - AC

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.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1058
3701
Doc:

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.

Default

The default file system is specified by the **cd** command. When you omit the **/all** keyword, the Cisco IOS 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.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1059
Fls:
3701
Doc:

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... eeee
```

E C
1.4.337-3
CPL - AC

```
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.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1060
Fls:
Doc: 3701

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.

ECT 4.335 J CPL - AC

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
```

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1061
Fls:
3701
Doc:

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.

ECT 1 4.333 1 CPL - AC J

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.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1062
Doc: 3701

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.

ECT
1.331
CPL - AC

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
```

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1063
Fls:
3701
Doc:

nkdir

To create a new directory in a Class C Flash file system, use the **mkdir** EXEC command.

mkdir *directory*

yntax Description

directory	The name of the directory to create.

ommand Modes

EXEC

ommand History

Release	Modification
11.3 AA	This command was introduced.

Jsage 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)
```

Rela ommands

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.

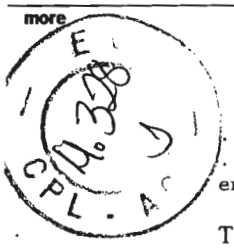
These commands show the version number of the software used when you last changed the configuration file.

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.

ename

To rename a file in a Class C Flash file system, use the **rename** EXEC command.

rename *url1 url2*

ntax Description

url1	The original path and filename.
url2	The new path and filename.

mmand Modes

EXEC

mmand History

Release	Modification
11.3 AA	This command was introduced.

sage Guidelines

This command is valid only on Class C Flash file systems.

xamples

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)
```

ECT 4.325 J CPL - AC

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.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1066
Doc: 3701

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:

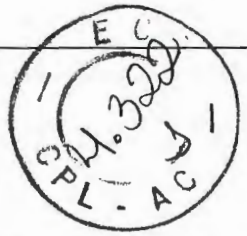
```
Router# show file descriptors

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.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1067
Fls:
Doc 3701



how file information

To display information about a file, use the **show file information** EXEC command.

show file information *file-url*

ntax Description

file-url	The URL of the file to display.

ommand Modes

EXEC

ommand History

Release	Modification
11.3 AA	This command was introduced.

xamples

The following is sample output from the **show file information** command:

```
Router# show file information tftp://dirt/hampton/c2500-j-1.a

tftp://dirt/hampton/c2500-j-1.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.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1068
Fls:
Doc: 3701

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.

ECT 14.319 CPL - AC

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.

ROS Nº 03/2005 - CN
CPMI - CORREIOS
1069
Fls:
Doc: 3701

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.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1071
Fls:
Doc: 3701

erify

To verify the checksum of a file on a Flash memory file system, use the **verify** EXEC command.

verify *filesystem*:[*file-url*]

ntax 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.

efaults

The current working device is the default device.

ommand Modes

EXEC

ommand History

Release	Modification
11.0	This command was introduced.

sage 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 does 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.

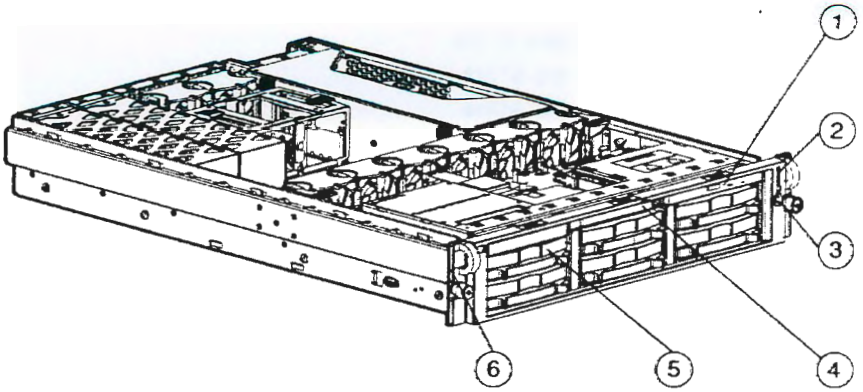
RQS Nº 03/2005 - CN
CPMI - CORREIOS
1073
Fls:
3701
Doc:

Apêndice CH

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1074
Doc: 3901

4309 J

Overview



1. 24X Max CD-ROM (with easy front ejection removol)
2. Front LEDs (show server status)
3. Unit Identification button and LED (for easy in rack server identification)
4. 1.44 MB (3.5") Floppy Disk Drive
5. Six 1" Wide Ultro3/Ultra320 SCSI hot plug hard drives and one AIT or 20/40-GB DAT hot plug tape drive
6. 2U form factor

What's New

- The ProLiant DL380 G3 is now available with the latest technologies delivering best-in-class performance
- Intel® Xeon 3.06GHz processors available in two versions to satisfy a variety of applications:
- 3.06 GHz with 512K L2 Cache
- 3.06 GHz with 512K L2 Cache and 1 MB L3 Cache
- 533MHz Front Side Bus
- 1GB (expandable to 12GB on all systems greater than 2.8GHz) of 2-way interleaved PC2100 DDR SDRAM, with Advanced ECC and Online Spare capabilities

Overview

- Windows® 2000 Model
- Integrated Lights-Out (iLO) Management standard on system board
- Five Peer PCI Architecture up to 3.06 GHz processors and a 533MHz Front Side Bus
- ServerWorks GC -LE Chipset
- Integrated Smart Array 5i Plus Controller with optional Battery-Backed Write Cache (BBWC) Enabler option kit
- Three available 64-bit PCI-X slots, including two hot pluggable 100MHz slots and one 133MHz slot
- Two NC7781 PCI-X Gigabit NICs (embedded)
- Support for up to six 1" Wide Ultra3/Ultra320 SCSI hot plug hard drives or for five hot plug hard drives and one AIT hot plug tape drive
- User configurable single/dual channel drive backplane
- Internal hot plug capacity 880.8 GB standard (6 x 146.8 GB 1" HD)
- 00-Watt Hot Plug Power Supply (with optional redundancy)
- Hot Pluggable Fans (with optional redundancy)
- Sliding rails and cable management arm for easy serviceability and in-rack tool-less access to major components
- Automatic Server Recovery (ASR), ROM Based Setup Utility (RBSU), Insight Manager 7, Status LEDs including system health and UID and SmartStart
- Protected by HP Services, including a three-year, Next Business Day, on-site limited Globol warranty and extended Pre-Failure Warranty, which covers processors, memory, and hard drives - Certain restrictions and exclusions apply. Consult the HP Customer Support Center at 1-800-345-1518 for details.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1075
Fls:
Doc: 3701

Standard Features

Processor *One of the following depending on Model:*	Intel Xeon Processor 3.06 GHz/533 MHz-1GB Intel Xeon Processor 3.06 GHz/533MHz -512KB Intel Xeon Processor 2.8 GHz/400MHz -512KB Intel Xeon Processor 2.4 GHz/400MHz -512KB	
Cache Memory	512-KB Level 2 cache 1-MB Level 3 cache	
Upgradability (per server)	Upgradable to dual processing	
Chipset	ServerWorks GC -LE Chipset 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:*	Standard	1GB of 2-way interleaved PC2100 DDR SDRAM running at 266MHz on 3.06GHz models with Advanced ECC and Online Spare capabilities
	Maximum	12 GB
	Standard	512 MB of 2-way interleaved capable PC2100 DDR SDRAM running at 200MHz on 2.8GHz models and lower, with Advanced ECC capabilities and Online Spare capabilities
	Maximum	6 GB
Network Controller	Two NC7781 PCI-X Gigabit NICs (embedded)	
Expansion Slots	I/O (3 Total, 3 available)	PCI Voltage:
	64-bit/100 MHz Hot Plug PCI 2 64-bit/133 MHz Non Hot Plug PCI 1	3.3 Volt or universal cards
Storage Controller	Smart Array 5i Plus Controller (integrated on system board) NOTE: For complete list of devices supported the Smart array 5i Controller see the following: http://www5.compaq.com/products/quickspecs/11063_na/11063_na.HTML	
Storage	Diskette Drives	1.44 MB
	CD-ROM	24x IDE CD-ROM (Universal Media Bay)
	Hard Drives	None NOTE: The system can be operated in single channel (using either the embedded Smart Array 5i Plus controller or a PCI-based controller) or dual channel (with the first 2 drives on 1 channel, driven by the Smart Array 5i Plus controller and 4 drives driven by either the Smart Array 5i Plus or a PCI-based controller).
	Maximum Internal Storage	880.8 GB (6 x 146.8 GB Ultra 320 1")

Standard Features

Interfaces	Serial	1
	Pointing Device (Mouse)	1
	Graphics	1
	Keyboard	1
	External SCSI (VHDCI)	1
	Network RJ-45	3 (1 for iLO)
	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 ovoiloble in English only.

Graphics	Integrated ATI Rage XL Video Controller with 8-MB SDRAM Video Memory
Form Factor	Rack (2U), (3.5-inch)

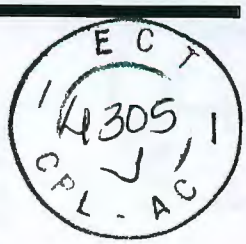
Standard Features

ProLiant Essentials Foundation Pack Software

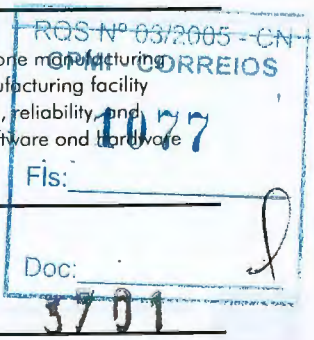
Insight Manager 7	Insight Manager 7 helps maximize system uptime and performance and reduces the cost of maintaining the IT infrastructure by providing proactive notification of problems before those problems result in costly downtime and reduced productivity. Insight Manager 7 is easy to set up and provides rapid access to detailed fault and performance information gathered by the Management Agents. One-click-access to the Integrated Lights-Out or Remote Insight Lights Out Edition 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.
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 Web site at: http://www.hp.com/servers/smartstart SmartStart version supported (minimum): SmartStart 6.0.
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, ond portables, and send alerts to Insight Manager 7 and other enterprise management opplications in case of subsystem or environmental failures. For additional information about the Management Agents and other management products from, HP please visit the management website at: http://www.hp.com/servers/manage
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 advonced 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 outomated solution for multi-server deployment and provisioning, enabling companies to quickly and easily adapt to changing business demands. • Workload Management Pock – 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. • Integrated Lights-Out Advanced Pack – upgrades the Integrated Lights-Out processor to full virtual presence and control with graphical console and virtual media. • Recovery Server Option Pack – entry-level high availability software that will provide reliable protection and increased uptime against server hardware and operating system failures. • 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 availoble 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.

Standard Features



Industry Standard Compliance	ACPI 1.0b Compliant PCI 2.2 Compliant WOL Support Microsoft® Logo certifications USB 1.1
Manageability	Insight Manager 7 Redundant ROM Remote Flash ROM Integrated Lights Out Support Management Agent Automatic Server Recovery (ASR) Remote Insight Lights-Out Edition II (optional) Integrated Management Log Drive Parameter Tracking (with Smart Array Controllers) Dynamic Sector Repairing (with Smart Array Controllers) Hot Spare Boot (NOTE: Upon the event of a failed processor or VRM in a multi-processing environment, the system will automatically reboot and use the remaining good processor(s).) Pre-Failure Warranty (covers processors, hard drives and memory)
Security	Power-on password Keyboard password Diskette drive control Diskette boot control QuickLock, Network Server Mode Serial interface control Administrator's password Disk configuration lock
Server Power Cords	One Lowline NEMA power cord and One Highline IEC Power cord ships standard
Power Supply	400 Watt, CE Mark Compliant Optional Hot Plug AC Redundant Power Supply and DC Redundant Power Supply
System Fans	5 fans ship standard. 8 total supported internally NOTE: The additional 3 fans are available via Option Kit (PN 293048-B21).
Required Cabling	For required cabling information, refer to the Web site at: http://www.compaq.com/products/servers/proliantDL380 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

OS Support

Microsoft Windows NT® Server
Microsoft Windows 2000
Novell NetWare
Caldera OpenUNIX 8
LINUX (Red Hat, SuSE)

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: For an up-to-date listing of the latest drivers available for the ProLiant DL380 G3, please see: http://www.compaq.com/support/files/server/us/index.html.
NOTE: For a more complete and up-to-date information on Linux support, please visit HP Linux Web site at: http://h18000.www1.hp.com/products/servers/linux/hpLinuxcert.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 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.compaq.com/products/servers/proliantdl380/index.html
NOTE: This Web site is available in English only.

Rack Kit

Tool-free support for racks with square mounting holes (including Compaq/HP 7000, 9000, 10000 and H9 series), with an adjustment range of 24" - 36".

Telco Rack Support

DL380 G3 Telco Rack Kit:
Support for all 2-post Telco racks requires the use of the standard rack kit and an additional option kit from Rack Solutions (http://www.racksolutions.com/hp)
NOTE: This Web site is available in English only.

ECT 4.303 CPLA

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.
NOTE: Factory Express Engineered Solution Level 6 is o custom solutions availoble through Factory Express. Please contact a your local reseller or Account Monager.

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. HP technical assistance is available 7x24, toll free in the United States and Canada. Telephone support services may be covered under warranty or available for an additional fee.

NOTE: Limited Warranty includes 3 year Parts, 3 year Labor, 3-year on-site support.

A full range of 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 information, customer/resellers can contact: 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 HP Customer Support Center at 1-800-345-1518 for details

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1078
Fls:
3701
Doc:

Models

DL380R03 X3.06-1MB/533, 1GB *333704-001*	Processor	(1) Intel Xeon Processor 3.06 GHz standard (up to 2 supported)
	Cache Memory	1-MB level 3 cache
	Memory	1 GB (Standard) to 12 GB (Maximum) of 2-way interleaved capable PC2100 DDR SDRAM running at 266MHz with Advanced ECC capabilities
	Network Controller	(2) NC7781 PCI-X Gigabit NIC (embedded)
	Storage Controller	Smart Array 5i Plus Controller (integrated on system board)
	Hard Drives	None ship standard
	Internal Storage	880.8 GB max (with optional hard drives)
	Optical Drive	24x IDE CD-ROM (Universal Media Bay)
	Form Factor	Rack (2U), (3.5-inch)
DL380R03 X3.06-512KB/533, 1GB *310[illegible]-001*	Processor	(1) Intel Xeon Processor 3.06 GHz standard (up to 2 supported)
	Cache Memory	512-KB level 2 cache
	Memory	1 GB (Standard) to 12 GB (Maximum) of 2-way interleaved capable PC2100 DDR SDRAM running at 266MHz, with Advanced ECC capabilities
	Network Controller	(2) NC7781 PCI-X Gigabit NIC (embedded)
	Storage Controller	Smart Array 5i Plus Controller (integrated on system board)
	Hard Drives	None ship standard
	Internal Storage	880.8 GB max (with optional hard drives)
	Optical Drive	24x IDE CD-ROM (Universal Media Bay)
	Form Factor	Rack (2U), (3.5-inch)
DL380R03 X2.8-512KB, 512MB, W2K *331441-001*	Processor	(1) Intel Xeon Processor 2.8 GHz standard (up to 2 supported)
	Cache Memory	512-KB level 2 cache
	Memory	512 MB (Standard) to 6 GB (Maximum) of 2-way interleaved capable PC2100 DDR SDRAM running at 200MHz, with Advanced ECC capabilities
	Network Controller	(2) NC7781 PCI-X Gigabit NIC (embedded) 10/100/1000 WOL (Wake on LAN) (embedded)
	Storage Controller	Smart Array 5i Plus Controller (integrated on system board)
	Hard Drives	None ship standard
	Internal Storage	880.8 GB max (with optional hard drives)
	Optical Drive	24x IDE CD-ROM (Universal Media Bay)
	Form Factor	Rack (2U), (3.5-inch)
	OS	Windows 2000 Server + 5 CALs standard with W2K model (not pre-installed)
DL380R03 X2.8-512KB/400, 512MB *301111-001*	Processor	(1) Intel Xeon Processor 2.8 GHz standard (up to 2 supported)
	Cache Memory	512-KB level 2 cache
	Memory	512 MB (Standard) to 6 GB (Maximum) of 2-way interleaved capable PC2100 DDR SDRAM running at 200MHz, with Advanced ECC capabilities
	Network Controller	(2) NC7781 PCI-X Gigabit NIC (embedded)
	Storage Controller	Smart Array 5i Plus Controller (integrated on system board)
	Hard Drives	None ship standard
	Internal Storage	880.8 GB max (with optional hard drives)
	Optical Drive	24x IDE CD-ROM (Universal Media Bay)
	Form Factor	Rack (2U), (3.5-inch)

Models

DL380R03 X2.4-512KB/400, 512MB *257917-001*	Processor	(1) Intel Xeon Processor 2.4 GHz standard (up to 2 supported)
	Cache Memory	512-KB level 2 cache
	Memory	512 MB (Standard) to 6 GB (Maximum) of 2-way interleaved capable PC2100 DDR SDRAM running at 200MHz, with Advanced ECC capabilities
	Network Controller	(2) NC7781 PCI-X Gigabit NIC (embedded)
	Storage Controller	Smart Array 5i Plus Controller (integrated on system board)
	Hard Drives	None ship standard
	Internal Storage	880.8 GB max (with optional hard drives)
	Optical Drive	24x IDE CD-ROM (Universal Media Bay)
	Form Factor	Rack (2U), (3.5-inch)

4.301
J
AC

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1079
Doc 3701

Options

ProLiant DL380 G3 Unique Options	DL380 G3 Redundant Fan Option Kit NOTE: Hot Plug Redundant Fan Option Kit (PN 293048-B21) contains three fans per kit.	293048-B21
	Hot Plug AC Redundant Power Supply Module (NEMA cord)	313054-001
	Hot Plug AC Redundant Power Supply Module (IEC cord)	313054-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
	ProLiant Essentials Workload Management Pack (Featuring Compaq Resource Partitioning Manager version 2.0)	303284-B21
	Flexible Quantity License Kit	302127-B21
	License-Only - for use with a Master License Agreement	302128-B21
	ProLiant Essentials Recovery Server Option Pack	280189-B21
	ProLiant Essentials Performance Management Pack v2.0, Single License	306696-B21
	ProLiant Essentials Integrated Lights-Out Advanced Pack	263825-B21
	(Featuring: sophisticated virtual administration features for ultimate control of servers in the data centers and remote sites)	
	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.	
Software	HP digital asset protection	302316-001
Processor	Intel Xeon X3.06-1GB/533MHz Processor Option Kit NOTE: The 3.06GHz processor option kits are not backwards compatible; they cannot be used to upgrade systems purchased with 2.4 or 2.8GHz processors.	333713-B21
	Intel Xeon 3.06 GHz-512KB/533MHz Processor Option Kit NOTE: The 3.06GHz processor option kits are not backwards compatible; they cannot be used to upgrade systems purchased with 2.4 or 2.8GHz processors.	257916-B21
	Intel Xeon 2.80 GHz-512KB/400MHz Processor Option Kit NOTE: This processor option kit (PN 257915-B21) is not forwards compatible; it cannot be used in systems purchased with 3.06GHz processors. This processor option kit supports the ProLiant ML370 G3 and ProLiant DL380 G3 servers.	257915-B21
	Intel Xeon 2.40 GHz-512KB/400MHz Processor Option Kit NOTE: This processor option kit (PN 257913-B21) is not forwards compatible; it cannot be used in systems purchased with 3.06GHz processors. This processor option kit supports the ProLiant ML370 G3 and ProLiant DL380 G3 servers.	257913-B21
Memory	512MB of Advanced ECC PC2100 DDR SDRAM DIMM Memory Kit (2 x 256 MB)	300678-B21
	1024MB of Advanced ECC PC2100 DDR SDRAM DIMM Memory Kit (2 x 512 MB)	300679-B21
	2048-MB of Advanced ECC PC2100 DDR SDRAM DIMM Memory Kit (2x1024 MB)	300680-B21
	4096MB of Advanced ECC PC2100 DDR SDRAM DIMM Memory Kit (2x 2048 MB) NOTE: The 4096MB of Advanced ECC PC2100 DDR Memory kit (300682-B21) can only be used in 3.06GHz and faster models.	300682-B21

Options

Optical Drives	Slimline DVD-ROM (8x24x) Option Kit (Servers)	264007-B21
	Slimline CD-RW/DVD-ROM Combo Option Kit	331903-B21
Hard Drives	*Ultra 320 SCSI – Universal Hot Plug*	
	36.4GB 10,000 rpm, U320 Universal Hard Drive, 1"	286713-B22
	72.8GB 10,000 rpm, U320 Universal Hard Drive, 1"	286714-B22
	146.8GB 10,000 rpm, U320 Universal Hard Drive, 1"	286716-B22
	18.2GB 15,000 rpm, U320 Universal Hard Drive, 1"	286775-B22
	36.4GB 15,000 rpm, U320 Universal Hard Drive, 1"	286776-B22
	72.8GB 15,000 rpm, U320 Universal Hard Drive, 1"	286778-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 Hard Drive QuickSpecs for Technical Specifications such as capacity, height, width, interface, transfer rate, seek time, physical configuration, and operating temperature:
U320 Hard Drive QS:
http://www5.compaq.com/products/quickspecs/11531_na/11531_na.HTML

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1080
Fls:
Doc: 3701

Storage Controllers	Battery Backed Write Cache Enabler Option Kit	255514-B21
	Smart Array 532 Controller	225338-B21
	Smart Array 5302/128 Controller	283552-B21
	Smart Array 5304/256 Controller	283551-B21
	Smart Array 6402/128 Controller	273915-B21
	Smart Array 5312 Controller	238633-B21
	Smart Array 641 Controller	291966-B21
	Smart Array 642 Controller	291967-B21
	RAID ADG Upgrade for Smart Array 5302	288601-B21
	Ultra3 Channel Expansion Module for Smart Array 5300 Controller	153507-B21
	128-MB Cache Module for Smart Array 5302 Controller	153506-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 Coche Module upgrade kit supports the Smart Array 6400 series controller only.	273913-B21
	64 MB Battery Backed Write Cache Enabler NOTE: This 64 MB BBWC supports the Smart Array 641 Controller and Smart Array 642 Controller.	291969-B21
	64-Bit/133-MHz Dual Channel Ultra320 SCSI Adapter	268351-B21
	64-Bit/66-MHz Dual Channel Wide Ultra3 SCSI Adapter, Alternate OS	284688-B21
	NOTE: Please see the following Controller or SCSI Adapter QuickSpecs for Technical Specifications such os 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/11063_na/11063_na.HTML (Smart Array 5i Plus) 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_na/11555_na.HTML (U320 Adapter)	

Communications	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
	NC6170 Dual Port PCI-X 1000SX Gigabit Server Adapter	313879-B21
	NC6770 PCI-X Gigabit Server Adapter, 1000-SX	244949-B21
	NC7131 Gigabit Server Adapter, 64-bit/66Mhz, PCI, 10/100/1000-T	158575-B21
	NC7132 10/100/1000-T Upgrade Module for NC3134	153543-B21
	NC7170 Dual Port PCI-X 1000T Gigabit Server Adapter	313881-B21
	NC7770 PCI-X Gigabit Server Adapter	244948-B21
	NOTE: Any NC31XX, NC61XX, NC71XX or NC77XX NIC can be used for redundancy with the embedded NC7781 Network Controller.	

Redundant Options	DC Power Supply for the DL380 (48V)	268290-B21
	NOTE: The ProLiant DL380 G3 ships standard with a 100-240 volt auto-switching AC power supply. Each 48-volt DC option kit (PN 268290-B21) contains one power supply. Therefore, to convert to redundant DC power supplies, two must be purchased.	

Options

Redundant Options	Hat Plug AC Redundant Pawer Supply Module (NEMA cord)	313054-001
	Hot Plug AC Redundant Power Supply Module (IEC cord)	313054-B21
Management Options	Remote Insight Lights-Out Edition II	227251-001
	NOTE: USB Virtual Media Not Supported.	
	NOTE: The RILOE II USB Virtual Media feature is not supported on the 2.40 and 2.80 GHz versions of the ProLiant DL380 G3 and ProLiant ML370 G3 servers. The RILOE II cannot be used to connect the local client floppy and CD devices as USB virtual devices to the remote server. All other RILOE II features are supported on these servers. The non-USB based RILOE II Virtual Floppy feature is still supported, allowing you to perform functions such as remote ROM upgrades and server deployment. The Virtual Floppy feature requires loading the floppy image in to the RILOE II. For more details, please refer to the user guide of the RILOE II.	
Se[illegible]	HP/Atalla AXL600L SSL Accelerator Cord for ProLiant Servers	524545-B21
	Compaq AXL300 Accelerator PCI Card (HW SSL Encryption) for ProLiant Servers	227933-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
	TFT5110R Flat Panel Monitor (Carbon)	281683-B21

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1081
Fls:
Doc: 3701

Options

Tape Drives

NOTE: External tape devices, including both tape drives and tape arrays/enclosures, can be directly connected to the VHDCI SCSI port located on the back of the server. Use of a SCSI adapter to connect these devices is optional, not required.

Internal and External DAT Tape Drives

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 Drives

HP StorageWorks DAT 72e 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 AIT Tape Drives

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, External (Carbon)	157767-002
HP StorageWorks Internal AIT 50-GB, Hot Plug (Carbon)	215487-B21
HP StorageWorks AIT 50-GB Tape Drive, 3U Rackmount	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 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

External DLT Tape Drives

HP StorageWorks External 20/40-GB DLT Drive (opal)	340744-B22

NOTE: Please see the 20/40-GB DLT Drive 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/10234_na/10234_na.HTML

HP StorageWorks 40/80-GB DLT Tape Drive, External (Carbon)	146197-B22
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

External LTO Ultrium Tape Drives

4295
Q1544A

HP StorageWorks Ultrium 215 Tape Drive for ProLiant, External (Carbon)

NOTE: Please see the HP StorageWorks Ultrium 215 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, External (Carbon) Q1516A

NOTE: Please see the HP StorageWorks LTO Ultrium 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/11415_na/11415_na.HTML

HP StorageWorks Ultrium 460 Tape Drive for ProLiant, External (Carbon) Q1519A

NOTE: Please see the HP StorageWorks Ultrium 460 Tape Drives for ProLiant 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/11530_na/11530_na.HTML

Internal and External SDLT Tape Drives

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 110/22-0GB 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, External (carbon) 257319-001

NOTE: Please see the SDLT 160/320-GB Tape Drive QuickSpecs for additional options such as adopters, 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

External DAT Autoloader

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 35 GB Autoloader, Rackmount (Carbon) 280349-001

NOTE: The Integrated Smart Array 5I Controller does not support the AIT 35-GB Autoloader.
NOTE: Please see the AIT 35-GB 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, Rackmount kit C9266R

Rackmount Tape Drive Kits

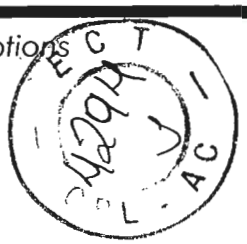
3U Rackmount Kit 274338-B21
NOTE: The 3U Rackmount Kit (PN 274338-B21) can support up to (2) full-height or (4) half-height tape drives and compatible with multiple Single-Ended and LVD SCSI Tape Drives including the 12/24-GB DAT, 20/40-GB DAT, AIT 35-GB LVD, AIT 50-GB, 20/40-GB DLT, 40/80-GB DLT, and the SDLT 110/220-GB 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 all DLT/SDLT tape drives including the 20/40-GB DLT, 35/70-GB DLT, 40/80-GB DLT, and the SDLT 110/220-GB tape drives.

NOTE: Please see the Rackmount Tape Drive Kits QuickSpecs for additional information regarding

REQ N° 03/2005 - CN
CPMI - CORREIOS
1082
Fls:
Doc: 3701

Options



these kits, please see the following:
http://www5.compaq.com/products/quickspecs/10854_no/10854_na.HTML

Rackmount Tape Drive 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 MSL6000 and MSL5000 Departmental tape libraries

MSL6060L1 - LTO Ultrium 1 based departmental library up to 4 drives and 60 slots

MSL6060, 0 DRV, Ultrium 460, RM Library 331196-B23

MSL6060, 2 DRV, Ultrium 460, RM Library 331196-B21

MSL6060, 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

MSL5060L1 - LTO Ultrium 1 based departmental library up to 4 drives and 60 slots

MSL5060, 0 DRV, Ultrium 230, RM Library 301899-B21

MSL5060, 2 DRV, Ultrium 230, RM Library 301899-B22

MSL5060, 2 DRV, Ultrium 230, embedded Fibre, RM Library 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, 0 DRV, SDLT 160/320, RM Library 255102-B21

MSL5052S2, 2 DRV, SDLT 160/320, RM Library 293474-B21

MSL5052S2, 2 DRV, SDLT 160/320, RM Library with embedded FC router option 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

MSL6030 - LTO Ultrium 1 based departmental library up to 4 drives and 60 slots

MSL6030, 0 DRV, RM Library 330731-B21

MSL6030, 1 DRV, LTO Ultrium 460, RM Library 330731-B22

MSL6030, 2 DRV, LTO Ultrium 460, RM Library 330731-B23

MSL6030, 1 DRV, LTO Ultrium 460, embedded Fibre, RM Library 330731-B24

MSL 6030, 2 DRV, LTO Ultrium 460, embedded Fibre, RM Library 330731-B25

NOTE: Please see the StorageWorks MSL6030 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/11625_na/11625_na.HTML

MSL5030L1 - LTO Ultrium 1 mid-range library up to 2 drives and 30 slots

MSL5030, 0 DRV, RM Library 301897-B21

MSL5030, 1 DRV, LTO Ultrium 230, RM Library 301897-B22

MSL5030, 2 DRV, LTO Ultrium 230, RM Library 301897-B23

MSL5030, 1 DRV, LTO Ultrium 230, embedded Fibre, RM Library 301897-B24

MSL 5030, 2 DRV, LTO Ultrium 230, embedded Fibre, RM Library 301897-B25

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, RM Library 293472-B21

E C T
4293
L AC

MSL5026S2, 1 DRV, SDLT 160/320, RM Library	293472-B22
MSL5026S2, 2 DRV, SDLT 160/320, RM Library	293472-B23
MSL5026S2, 1 DRV, SDLT 160/320, RM Library with embedded FC router option	293472-B24
MSL5026S2, 2 DRV, SDLT 160/320, RM Library with embedded FC router option	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 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

MSL5026SL Opal - SDLT110 based mid-range library up to 2 drives and 26 slots

MSL5026, 0 DR, LVD, RM	231979-B21

MSL5026DLX- 40/80GB DLT based mid-range library up to 2 drives and 26 slots

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

MSL5000 SDLT 160/320 Upgrade DRV (MSL5052S2 & MSL5026S2 only)	293475-B21
MSL Ultrium 460 upgrade drive in hot plug canister	
MSL5000 LTO Ultrium 1 Upgrade DRV (MSL5060L1 & MSL5030L1 only)	301901-B21
MSL5000 SDLT 110/220 Upgrade DRV	231823-B22
MSL5000 40/80GB DLT Upgrade DRV	231823-B21
MSL5000 Dual Magazine LTO (2 X 15 slot magazines)	301902-B21
MSL5000 Dual Magazine DLT (2 X 13 slot magazines)	232136-B21
MSL Universal passthrough mechanism	304825-B21
MSL5026, 5U Pass through extender (required one for each unit connected to the stack, for third and additional units) - for MSL5026 & MSL5030	231824-B22
MSL5052, 10U Pass-Through Extender (required one for each unit connected to the stack, for third and additional units) - for MSL5052 & MSL5060	231824-B23

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

RDS N° 175197-B21 - CN
CPMI - 175198-B21 OS
1083
Fls: 3701
Doc:

Options

Smart Array Cluster Storage	Smart Array Cluster Storage	201724-B21
	Smart Array Cluster Storage Redundant Controller Option Kit	218252-B21
	4-Port Shared Storage Module with Smart Array Multipath Software for Smart Array Cluster Storage	292944-B21
	128-MB Cache Module for Smart Array 5302 Controller	153506-B21
	NOTE: 128-MB Cache Module for Smart Array 5302 Controller (PN 153506-B21) is an upgrade cache module (128 MB Standard) for Smart Array Cluster Storage Controller.	
	256-MB Battery-Backed Cache Module	254786-B21
	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	
Cluster Options	ProLiant Cluster HA/F100 for MSA1000 v2	252408-B22
	ProLiant Cluster HA/F200 for MSA1000 v2	252409-B22
	NOTE: For additional information regarding the ProLiant Cluster for HA/F100, HA/F200 for MSA1000 please see the following QuickSpecs at: http://www5.compaq.com/products/quickspecs/11035_na/11035_na.html	
	ProLiant Cluster HA/F500 Enhanced Kit for Enterprise Virtual Array	254623-B22
	ProLiant Cluster HA/F500 Basic Kit for Enterprise Virtual Array	313047-B21
	NOTE: For additional information regarding the ProLiant Cluster for HA/F100, HA/F200 for MSA1000 please see the following QuickSpecs at: http://www5.compaq.com/products/quickspecs/11055_na/11055_na.html	
	ProLiant Cluster HA/F500 for MA8000 Basic Kit	103250-B26
	ProLiant Cluster HA/F500 for MA8000 Enhanced Kit	379937-B26
	ProLiant Cluster HA/F500 for MA8000 Enhanced DT Kit	164227-B24
	NOTE: For additional information regarding the ProLiant Cluster for HA/F500 for MSA8000 please see the following QuickSpecs at: http://www5.compaq.com/products/quickspecs/10232_na/10232_na.html	
	ProLiant Cluster HA/L100 – LifeKeeper for Linux	303523-B22
	NOTE: For additional information regarding the ProLiant Cluster HA/L100 LifeKeeper for Linux, please see the following QuickSpecs at: http://www5.compaq.com/products/quickspecs/11533_na/11533_na.html	
	HP Serviceguard for Linux ProLiant Cluster NOTE: Kit includes 2 licenses, documentation and an Ethernet crossover cable.	305199-B21
	HP Serviceguard for Linux License NOTE: Kit includes single license version and documentation.	307554-B21
	NOTE: For additional information regarding the HP Serviceguard for Linux License, please see the following QuickSpecs at: http://www5.compaq.com/products/quickspecs/11518_na/11518_na.html	
External Storage - Rack	StorageWorks Enclosure Model 4314R (rack-mountable)	190209-001
	StorageWorks Enclosure Model 4354R (rack-mountable)	190211-001
	NOTE: The StorageWorks Enclosure 4300 Family supports the Wide Ultra3, Ultra320 1" Hot Plug Hard Drives.	
	StorageWorks Enclosure 4200 Redundant Power Supply Option	119826-B21
	StorageWorks Enclosure 4200 Ultra3 Single Bus I/O Module Option	190212-B21
	StorageWorks Enclosure 4200 Ultra3 Dual Bus I/O Module Option	190213-B21
	StorageWorks Enclosure Tower to Rack Conversion Kit	150213-B21

Options

MSA1000	MSA1000	201728-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	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 Modular Array 8000/Enterprise Modular Array 12000	EMA12000 D14 60Hz	175990-B21
	EMA12000 S14 60Hz	175991-B21
	MA8000 60Hz	175992-B21
	EMA12000 Blue 60Hz	175993-B21
	NOTE: Options include controller, solution kits, ACS. MA8000/EMA12000 includes controller shelf, drive shelves and cabinet. Packaging upgrade to RA8000/ESA12000.	
	NOTE: Please see the StorageWorks MA8000/EMA12000 QuickSpecs for FC Hubs, FC switches, platform software, host adapters, disks and options for complete solutions at: http://www5.compaq.com/products/quickspecs/10545_na/10545_na.HTML	
StorageWorks Enterprise Modular Array 16000 FC	EMA16000 D14 60Hz (opal)	238792-B21
	EMA16000 S14 60Hz (opal)	238791-B21
	NOTE: Models include: Duol HSG80 controllers in each Model 2200 enclosure (2 pairs per single bus configuration, 4 pairs per dual bus configuration) with 1GB cache per controller pair, and 12 14-bay drive enclosures with redundant power supplies. Configure-to-Order (CTO) builds are available. Options include ACS, platform kits and software by HP.	
	NOTE: Please see the StorageWorks EMA16000 QuickSpecs for FC switches, platform software, host adapters, disks and options for complete solutions at: http://www5.compaq.com/products/quickspecs/10812_na/10812_na.HTML	
StorageWorks Options	StorageWorks Director 2/64	286809-B21
	NOTE: Please see the StorageWorks Director 2/64 QuickSpecs for additional information: http://www5.compaq.com/products/quickspecs/11003_na/11003_na.HTML	
	StorageWorks SAN Switch 2/8-EL	322120-B21
	StorageWorks SAN Switch 2/8-EL Upgrade	325888-B21
	StorageWorks SAN Switch 2/16	322118-B21
	StorageWorks SAN Switch 2/16-EL Upgrade	288250-B21

4291 J
RQS Nº 03/2005 - CN
CPMI - CORREIOS
1084
Fls: 3701
Doc:

Options

UPS and RDU 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 – Rack	HP UPS R1500 XR (1440VA, 1340 Watt), Low Voltage	204404-001
	HP UPS R3000 XR (2880VA, 2700 Watt), Low Voltage	192186-001
	HP UPS R3000 XR (3000VA, 2700 Watt), High Voltage	192186-002
	Rack-Mountable UPS R6000 (6000VA, 6000 Watt) High Voltage	347207-001
	HP UPS R12000 XR N+x (200-240V) (hardwired)	207552-B22
	NOTE: UPS R6000 has a hardwired input; and the UPS R12000 XR has a hardwired input and output connection.	
UPS Options	SNMP Serial Port Card	192189-B21
	NOTE: Supports tower and rack UPS XR models. This card does not support the 500, 700, and 6000VA UPSs (non-XR models)	
	Six Port Card	192185-B21
	NOTE: Supports tower and rack UPS XR models. This card does not support the 500, 700, and 6000VA UPSs (non-XR models)	
	High to Low Voltage Transformer (250VA)	388643-B21
	NOTE: Supports R6000 UPS series only. 2.5 amps @ 125 Volts max output across two NEMA 5-15.	
	Extended Runtime Module, R1500 XR, 2U	218971-B21
	NOTE: 2U each, two ERM maximum.	
	Extended Runtime Module, R3000 XR, 2U	192188-B21
	NOTE: 3U each, one ERM maximum.	
	Extended Runtime Module, R6000, 3U	347224-B21
	NOTE: 3U each, two ERM maximum.	
	Extended Runtime Module, R12000 XR, 4U	217800-B21
	NOTE: 4U each, one ERM maximum.	
	R12000 XR BackPlate Receptacle Kit, (2) L6-30R	325361-001
	NOTE: The R12000 XR BackPlate Kit has a hardwired input.	
	R12000 XR BackPlate Receptacle Kit, (2) IEC-309R	325361-B21
	NOTE: The R12000 XR BackPlote Kit has a hardwired input.	
	SNMP-EN Adapter	347225-B21
	NOTE: Supports R6000 UPS series only.	
	Multi-Server UPS Card	123508-B21
	NOTE: Supports R6000 UPS series only.	
	Scalable UPS Card	123509-B21
	NOTE: Supports R6000 UPS series only.	

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 For North America, need to order cable PN 340653-001.	
	NOTE: Please see the following Modular Power Distribution Unit (Zero-U/1U Modular PDUs) QuickSpecs for additionol 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 Mounting Kit NOTE: This kit allows you to mount the Modular PDUs in racks other than the 9000/10000 Series racks (ony racks using the standard 19"rail). 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 (corbon)	195255-B25
	USB 2-Button Scroll Mouse (carbonite)	DC172B
	USB Floppy	304707-B21
Rack Builder	Please see the Rack Builder for configuration assistance at http://www.compaq.com/rackbuilder/	

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1085
Fls:
3701
Doc:

Options

HP Rack 10000 Series (Graphite Metallic)	HP S10614 (14U) Rack Cabinet - Shock Pallet	292302-B22
	HP 10842 (42U, 800mm wide) – Pallet	257415-B21
	HP 10842 (42U, 800mm wide) – 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.	
	NOTE: Please see the Rack 10000 QuickSpecs for Technical Specifications such as height, width, depth, weigh, 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.	
Rack 9000 Series (opal)	Rack 9142 (42U) – Pallet	120663-B21
	Rack 9142 (42U) – Shock Pallet	120663-B22
	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.html NOTE: This Web site is available in English only.	

E C T
4287
CPL AC

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).	
	800mm Wide Stabilizer Kit (Graphite)	255488-B21
	NOTE: Supported by the Rack 10842 cabinet only.	
	600mm Stabilizer Kit – Graphite	246107-B21
	Baying Kit for Rack 10000 series (Carbon)	248929-B21
	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-options/index.html	
	NOTE: This Web site is available in English only.	

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1086
Fls:
Doc: 3701

Options

Rack Options for 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 Campaq 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.	
	9142 Split Rear Door	254045-B21
	NOTE: The 9142 Split Rear Door (PN 254045-B21) supports the 600 mm wide, 42U 9000 series rack.	
	9136 Extension Kit	218216-B21
	9142 Short Rear Door	218217-B21
	NOTE: The 9142 Short Rear Door (PN 218217-B21) supports the Compaq Rack 9142 only.	
	9136 Short Rear Door	218218-B21
	Rack Blanking Panel (Multi)	169940-B21
	NOTE: Kit includes four panels in 1U, 2U, 4U, and 8U.	
	Rack Blanking Panels (1U)	189453-B21
	NOTE: The Rack Blanking Panels (PN 189453-B21) contains 10 each of (1U).	
	Rock Blanking Panels (2U)	189453-B22
	NOTE: The Rack Blanking Panels (PN 189453-B22) contains 10 each of (2U).	
	Rack Blanking Panels (3U)	189453-B23
	NOTE: The Rack Blanking Panels (PN 189453-B23) contains 10 each of (3U).	
	Rack Blanking Panels (4U)	189453-B24
	NOTE: The Rack Blanking Panels (PN 189453-B24) contains 10 each of (4U).	
	Rack Blanking Panels (5U)	189453-B25
	NOTE: The Rack Blanking Panels (PN 189453-B25) contains 10 each of (5U).	
	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 hordware for connecting racks and a ponel to cover the 100mm gap at the rear of the two racks.	
	NOTE: For additionol 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 Rack 7000 Series	High Air Flow Rack Door Insert for 7122	157847-B21
	High Air Flow Rack Door Insert for 7142	327281-B21
	High Air Flow Rack Door Insert for 7142 (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.	
Rack Options for Rack	Monitor Utility Shelf- opal	303606-B21

E C T
4289
L JA C

Options

7000, 9000 and 10000 Series	Ballast Option Kit	120672-B21
	Rack Rail Adapter Kit (25" depth)	120675-B21
	100 kg Sliding Shelf	234672-B21
	Monitor/Utility Shelf - Graphite	253449-B21
	Depth Adjustable Fixed Rail	332558-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 (100-230 VAC)	120206-001
	Server Console Switch 1 x 4 port (100-230 VAC)	400336-001
	Server Console Switch 1 x 8 port (100-230 VAC)	400337-001
	Server Console Switch 2 x 8 port (100-230 VAC)	400338-001
	Server Console Switch 2 x 8 port (48VDC)	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 (115V)	144007-001
	Switch Box Connector Kit (230V)	144007-002
	TFT5600 Rack Keyboard Monitor	221546-001
	Local Access Cable Kit	232985-B21
	1U Rack Keyboard & Drawer (Carbon) NOTE: The 1U Rack Keyboard & Drawer (PN 257054-001) is to be used with the Keyboards for Racks with Trackball (PN 158649-001).	257054-001
	Input Device Adjustable Roils NOTE: Input Device Adjustable Rails (287139-B21) are for use with the TFT5110R, TFT5600RKM and integrated keyboard/drawer which is used in mounting into third party racks.	287139-B21
	Input Device Telco Rail NOTE: Input Device Adjustable Rails (287138-B21) are for use ONLY with the TFT5110R, TFT5600RKM ond integrated keyboard/drawer which is used in mounting into third porty racks.	287138-B21
	Keyboard/Monitor/Mouse extension cables NOTE: For additional information regarding Rack Options, please see the following URL: http://h18000.www1.hp.com/products/servers/proliantstoroge/rack-options/index.html NOTE: This Web site is available in English only.	149989-001

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1087
Fls: 3701
Doc:

Options

Rack Options for Third-Party Cabinet Racks	Round hole rack cabinet rail kit NOTE: Support for racks with round mounting holes (include HP Rack System /E and HP Systems) with an adjustment range of 24"- 36".	293052-B21

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 oddressing, 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 arroy, Start-up installation services custom quote. (price/rack). NOTE: Factory Express Engineered Solution Level 6 is a custom solutions availoble 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 4-Hour On-site Service*	
	4-Hour On-site Service 5-Day x 13-Hour Coverage, 3 Years (Canadian Part Number)	FP-LO3EC-36
	4-Hour On-site Service, 5-Day x 13-Hour, 3 Years (U.S. Part Number)	331066-002
	4-Hour On-site Service, 7-Day x 24-Hour Coverage, 3 Years (Canadian Part Number)	FP-LO7EC-36
	4-Hour On-site Service, 7-Day x 24-Hour Coverage, 3 Years (U.S. Part Number)	162657-002
	Installation & Start-up Services	
	Hardware Installation (Canadian Part Number)	FP-LOINS-EC
	Hardware Installation (U.S. Part Number)	401792-002

ECT
4283
LJ AC

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)	240014-002
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-02
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)	331072-002
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-02
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 discretian, 8am-9pm, M-F 2hr response time excl. HP holidays. (Canadian Part Number)	FM-M01E2-36
Onsite HW support, 8am-9pm, M-F, 4hr response and Linux O/S SW Tech support offsite, onsite at HP's discretian, 8am-9pm, M-F 2hr response time excl. HP holidays. (U.S. Part Number)	331070-002
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-L01E2-36
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)	239931-002
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-M02E2-36
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)	331071-002
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-L02E2-36
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-M04E2-36
24 x 7 HW, 4-hr response, Named HW engineer; 24 x 7 Silver Subsequent System Support for Windaws NT, Windows 2000, Professional, Server or Advanced Server Operating System (2-5-2 Part Number for Canada)	FM-M24E2-36
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-N04E2-36
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-N24E2-36
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.)	239933-002
24 x 7 HW, 4-hr response, Named HW engineer; 24 x 7 Silver Subsequent System Support for Windows NT, Windaws 2000, Professional, Server or Advanced Server Operating System (6-3 Part Number for U.S.)	239935-002
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.)	239973-002

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1088
Fls: 3701
Doc:

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.)	239975-002

NOTE: For more information, customer/resellers can contact http://www.hp.com/services/carepack

Memory

HP ProLiant Model DL380 Generation 3 (G3) 3.06GHz Models

Standard Memory

1 GB PC2100 Registered DDR SDRAM DIMM Memory running at 266MHz comes installed (2 x 512-MB SDRAM)

Standard Memory Plus Optional Memory

Up to 9,216-MB memory is available with the optional installation of PC2100 Registered DDR SDRAM DIMM Memory Option Kit

Standard Memory Replaced with Optional Memory

Up to 12,288-MB of memory is available with the removal of the standard 512-MB of memory and the optional installation of PC2100 Registered DDR SDRAM DIMM Memory Option Kit

NOTE: Chart does not represent all possible configurations.

Memory		Slot					
		1	2	3	4	5	6
Standard	1024MB	512MB	512MB	Empty	Empty	Empty	Empty
Optional	8,960MB	512MB	512MB	2048MB	2048MB	2048MB	2048MB
Maximum	12,288MB	2048MB	2048MB	2048MB	2048MB	2048MB	2048MB

NOTE: In the online spare configuration, the ROM automatically configures the last populated back as the spare memory. If only banks A and B are populated, bank B is the spare bank. If banks A, B, and C are populated, bank C is the spare bank, Online spare memory is configured through RBSU.

Following are memory options available from HP:

- 4096MB of Advanced ECC PC2100 DDR SDRAM DIMM Memory Kit (2x 2048 MB) 300682-B21
  NOTE: The 4096MB of Advanced ECC PC2100 DDR Memory kit (300682-B21) can only be used in 3.06GHz and faster models.
- 2048-MB of Advanced ECC PC2100 DDR SDRAM DIMM Memory Kit (2x1024MB) 300680-B21
- 1024-MB of Advanced ECC PC2100 DDR SDRAM DIMM Memory Kit 2 x 512MB) 300679-B21
- 512-MB of Advanced ECC PC2100 DDR SDRAM DIMM Memory Kit (2 x 256MB) 300678-B21

HP ProLiant Model DL380 Generation 3 (G3) 2.8GHz and 2.4GHz Models

Standard Memory

512-MB PC2100 Registered DDR SDRAM DIMM Memory running at 200MHz comes installed (2 x 256-MB SDRAM)

Standard Memory Plus Optional Memory

Up to 4,608-MB memory is available with the optional installation of PC2100 Registered DDR SDRAM DIMM Memory Option Kit

Standard Memory Replaced with Optional Memory

Up to 6,144-MB of memory is available with the removal of the standard 256-MB of memory and the optional installation of PC2100 Registered DDR SDRAM DIMM Memory Option Kit

NOTE: Chart does not represent all possible configurations.

Memory		Slot					
		1	2	3	4	5	6
Standard	512MB	256MB	256MB	Empty	Empty	Empty	Empty
Optional	4,608MB	256MB	256MB	1024MB	1024MB	1024MB	1024MB
Maximum	6,144MB	1024MB	1024MB	1024MB	1024MB	1024MB	1024MB

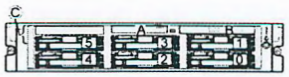
RDS Nº 05/2005 - CN
CPMI - CORREIOS
1089
Fls: 3701
Doc:

Memory

NOTE: In the online spare configuration, the ROM automatically configures the last populated back as the spare memory. If only banks A and B are populated, bank B is the spare bank. If banks A, B, and C are populated, bank C is the spare bank, Online spare memory is configured through RBSU.

Following are memory options available from HP:

- 2048-MB of Advanced ECC PC2100 DDR SDRAM DIMM Memory Kit (2x1024MB) 300680-B21
- 1024-MB of Advanced ECC PC2100 DDR SDRAM DIMM Memory Kit 2 x 512MB) 300679-B21
- 512-MB of Advanced ECC PC2100 DDR SDRAM DIMM Memory Kit (2 x 256MB) 300678-B21



0 - 5	Six 6" Wide Ultra3 SCSI hot plug hard drive bays
A	1.44-MB Diskette Drive
B	24x IDE CD-ROM (Universal Media Bay)
C	Six 1" Wide Ultra3/Ultra320 SCSI hot plug hard drives or for five hot plug hard drives and one AIT or 20/40-GB DAT hot plug tape drive

Drive Support

Removable Media

	Quantity Supported	Position Supported	Controller
1.44-MB Diskette Drive	1	A	Integrated
IDE CD-ROM Drive	1	B	Integrated IDE
Slimline DVD-ROM (8x24x) C Kit (Servers)	1	B	Integrated IDE

Hard Drives

Ultra320 Hot Pluggable Drives

	Quantity Supported	Position Supported	Controller
1-inch	Up to 6	0-5	Smart Array 5i Controller (integrated on system board)
146.8-GB 10,000 rpm			Smart Array 532 Controller
72.8-GB 10,000 rpm			Smart Array 5302/128 Controller
36.4-GB 10,000 rpm			Smart Array 5304/256 Controller
72.8-GB 15,000 rpm			Smart Array 6402/128 Controller
36.4-GB 15,000 rpm			Smart Array 5312 Controller
18.2-GB 15,000 rpm			Smart Array 641 Controller
			Smart Array 642 Controller
			64-Bit/133-MHz 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.

External Storage

	Quantity Supported	Position Supported	Controller
StorageWorks Enclosure 4300 Family (supports Ultra2/Ultra3 1" drives only)	Up to 13	External	Smart Array 532 Controller Smart Array 5302/128 Controller Smart Array 5304/256 Controller Smart Array 6402/128 Controller Smart Array 5312 Controller Smart Array 642 Controller 64-Bit/133-MHz Dual Channel Ultra320 SCSI Adapter
3U Rackmount Kit 5U Rackmount Kit	Up to 3	External	64-Bit/133-MHz 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

ROS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1090
Doc:
3791

Storage

Maximum Storage Capacity – (StorageWorks Enclosure SCSI Attached)

Internal	880.8 GB (6 x 146.8 GB Ultra 320 1")
External	26.717 TB (13 x (14 x 146.8 GB Ultra 320 1"))
Total	27.598 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 on 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

NOTE: Please see the Smart Array 5i Controller QuickSpecs for additional information regarding supported options at:
http://www5.compaq.com/products/quickspecs/10890_NA/10890_NA.HTML

	Quantity Supported	Position Supported	Controller
Internal DAT 20/40 Internal DAT 72	Up to 3	0+1, 2+3, C	Smart Array 5i Controller (integrated on system board) Smart Array 532 Smart Array 5302/32 Controller Smart Array 5302/64 Cantroller Smart Array 5302/128 Controller Smart Array 5304/128 Controller Smart Array 5304/256 Controller Smart Array 6402/128 Controller Smart Array 5312 Controller 64-Bit/133-MHz Dual Channel Ultra320 SCSI Adapter
Internal AIT 100-GB, Hot Plug Internal AIT 50-GB, Hot Plug Internal AIT 35-GB, LVD, Hot Plug Internal 20/40-GB DAT, Hot Plug	Up to 3	0+ 1, 2+ 3, C	Smart Array 5i Controller Smart Array 532 Controller Smart Array 5302/128 Controller Smart Array 5304/256 Cantroller Smart Array 6402/128 Controller Smart Array 5312 Controller Smart Array 641 Controller Smart Array 641 Controller 64-Bit/133-MHz Dual Channel Ultra320 SCSI Adapter NOTE: The Smart Array 532 Controller does not support the AIT 100-GB Hot Plug Tape Drive.
2[illegible]-GB DAT DDS-4 8 Cassette Autoloader (external)	Up to 2	External	64-Bit/133-MHz Dual Channel Ultra320 SCSI Adapter
SSL1016 SDLT160/320 tape autoloader	Up to 2	External	64-Bit/133-MHz Dual Channel Ultra320 SCSI Adapter
HP StorageWorks AIT 35 GB Autoloader	Up to 1 (for a single HBA) Up to 2 (for a dual HBA)	External	64-Bit/133-MHz Dual Channel Ultra320 SCSI Adapter
Ultrium 215, External Ultrium 230, External Ultrium 460, External	Up to 2	External	64-Bit/133-MHz Dual Channel Ultra320 SCSI Adapter
SDLT 110/220-GB, External SDLT 160/320-GB, External	Up to 2	External	64-Bit/133-MHz 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	64-Bit/133-MHz Dual Channel Ultra320 SCSI Adapter
External 40/80-GB DLT Enhanced	Up to 3	External	64-Bit/133-MHz Dual Channel Ultra320 SCSI Adapter

SSL2020 AIT Library	Up to 5	External	SAN Access Module for Smart Array 5302 Controller 64-Bit/133-MHz Dual Channel Ultra320 SCSI Adapter
MSL5026DLX (40/80GB DLT-based) MSL5026SL (SDLT-based) Library MSL5052SL (SDLT-based) Library MSL5030L (LTO-based) Library MSL5060S (LTO-based) Library MSL6060L1 (Ultrium 460 - based) Library MSL6030 (LTO Ultrium - based) Library	2 drives per SCSI channel	External	64-Bit/133-MHz Dual Channel Ultra320 SCSI Adapter

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1091
Fls:
Doc: 3701

Power Specifications

Part Number	194989-001
Spare Kit	199382-B21
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	400	400	400	400	400	400
Nominal Input Current (A rms)	5.8	5.0	2.7	2.5	2.4	2.3
Max Rated Input Wattage Rating (Watts)	571	563	548	541	541	541
Max. Rated VA (Volt-Amp)	583	575	559	552	552	552
Efficiency (%)	70	71	73	74	74	74
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)	50	50	50	50	50	50
Maximum Inrush Current duration	20	20	20	20	20	20

System Specifications

ProLiant DL380 Generation 3 Fully Configured

Up to 2 Processors, 6 Memory Slots, 6 Hard Drives, 3 PCI Slots, and 2 Hot Plug Power Supplies

Nominal Input Voltage (Vrms)	100	115	208	220	230	240
Fully Loaded System Input Wattage (W)	431	411	406	400	395	390
Fully Loaded System Input Current (A rms)	4.3	3.6	2.0	1.9	1.8	1.7
Fully Loaded System Thermal (BTU- Hr)	1421	1401	1383	1365	1347	1330
Fully Loaded System VA (Volt-Amp)	425	419	414	408	403	398
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)	100	100	100	100	100	100
Power cord requirements	Nema 5-15P to IEC320-C13			Option no./Spare no.: See Chart below		
	IEC320-C13 to IEC320-C14			Option no./Spare no.: 142259-001/142258-B21		

Notes:

* To view typical system power ratings use the Active Answers Power Calculator which is available via the online tool located at URL: http://h30099.www3.hp.com/configurator/powercalcs.asp

To drill down to calculators:

- Click on: "ProLiant Servers"
- Click on the Server of interest. Example: DL380 G3
- Click on: "Power Calculator" link. (You may need to scroll down to see it.)

Power Cords (Nema 5-15P to IEC320-C13)	
Country	
Standard Power Cord Part Number/Option Power Cord Part Number	163719-002/227099-001
Power Cords (IEC320-C13 to IEC320-C14)	
Standard Power Cord Part Number/Option Power Cord Part Number	142263-003/142257-003

E C T
14275
L. A.

System Unit	Dimensions (HxWxD)	3.38 x 17.50 x 25.75 in (8.59 x 44.45 x 65.41 cm)	
	Weight	Maximum:	60 lb (27.22 kg)
		No drives:	47.18 lb (20.41 kg)
	Input Requirements (per power supply)	Range Line Voltage	90 to 132 VAC/180 to 265 VAC
		Nominal LineVoltage	100 to 120 VAC/220 to 240 VAC
		Rated Input Current	6A (110V) to 3A (220V)
		Rated Input Frequency	50 to 60 Hz
		Rated Input Power	600W
	BTU Rating	1,475 BTU/HR	
	SCSI Connectors	One external VHDCI connector	
	Power Supply Output Power (per power supply)	Rated Steady-State Power	400W
		Maximum Peak Power	400W
	Temperature Range	Operating	50° to 95° F (10° to 35° C)
		Shipping	-40° to 158° F (-40° to 70° C)
	Relative Humidity (non-condensing)	Operating	10% to 90%
		Shipping	5% ta 95%
	Maximum Wet Bulb Temperature	82.4° F (28° C)	
	Acoustic Noise	Idle Minimum (Fixed Disk Drives Spinning)	
		L WAd (BELS)	7.0
		L pAm (dBA)	55
		Operating Minimum (Random Seeks to Fixed Disks)	
		L WAd (BELS)	7.0
		L pAm (dBA)	55
	Acoustic Noise	Idle Maximum (Fixed Disk Drives Spinning)	
		L WAd (BELS)	7.2
		L pAm (dBA)	56
		Operating Maximum (Random Seeks to Fixed Disks)	
		L WAd (BELS)	7.3
		L pAm (dBA)	57

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1092
Fls: 3701
Doc:

1.44-MB Diskette Drive	Size	3.5 in	
	LED Indicators (front panel)	Green	
	Read/Write Capacity per Diskette (high/mid/low density)	1.44 MB/1.2 MB/720 KB formatted	
	Drive Supported	One	
	Drive Height	0.50 in (1.27 cm)	
	Drive Rotation	300/360/300 rpm	
	Transfer Rate (high/mid/low)	500/500/250 KB/s	
	Bytes/Sector	512	
	Sectors/Track (high/mid/low)	18/15/9	
	Tracks/Side (high/low)	80/80	
	Access Times	Track-to-Track (highmid//low)	3/3/6 ms
		Average (high/mid/low)	174/94/94 ms
		Settling Time	15 ms
		Latency Average	100 ms /83.3 ms /100 ms
	Cylinders (high/low)	80/80	
	Read/Write Heads	Two	

ECT 4273

24X Max IDE CD-ROM Drive (Universal Media Bay)	Disk	Applicable Disk	CD-DA, CD-ROM (Mode 1 and 2) CD-XA, CD-I (Mode 2, Form 1and 2) CD-I Ready, CD Extra, Video CD, CD-Bridge Photo CD (Single and Multi-session) CD-WO
		Capacity	550 MB (Mode 1, 12 cm) 640 MB (Mode 2, 12 cm)
		Diameter	4.7 in, 3.15 in/12in, 8 cm
		Rotational Speed	4200 rpm maximum
		Center Hole	0.6 in/1.524 cm diameter
		Thickness	0.047 in/0.12 cm
		Track Pitch	1.6 µm
	Block Size	Mode 0	2,368, 2,352 bytes
		Mode 1	2,352, 2,340, 2,336, 2,048 bytes
		Mode 2	2,352, 2,340, 2,336, 2,048 bytes
	Interface	IDE (ATAPI)	
	Access Times (typical)	Random	< 140 ms
		Full-Stroke	< 300 ms
	Data Transfer Rate	Sustained	150 KB/s (sustained 1X)
		Burst	2100 to 4800 KB/s
	Cache Buffer	128 KB	
	Start-up Time (typical)	< 10 seconds	
	Stop Time	< 5 seconds	
	Operating Conditions	Temperature	41° to 120° F (5° to 55° C)
		Humidity	10% to 80%
	Dimensions	(HxWxD, maximum)	0.51 x 5.24 x 5.2 in (1.3 x 13.31 x 13.21 cm)
		Weight	< 340 g

REQ. Nº 03/2005 - CN
CPMI - CORREIOS
1093
Fls: 3701

NC7781 PCI-X Gigabit NIC (embedded) 10/100/1000 WOL (Wake On LAN)	Network Interface	10Base-T/100Base-TX/1000 BaseTX	
	Compatibility	IEEE 802.3/802.3u compliant	
	Data Transfer Method	64-bit bus-master PCI-X	
	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 (Half-Duplex)	1000 Mb/s
		1000Base-TX (Full-Duplex)	2000 Mb/s
	Connector	RJ-45	
	Cable Support	10Base-T	Categories 3, 4 or 5 UTP; up to 328 ft (100 m)
		100Base-TX	Category 5 UTP; up to 328 ft (100 m)
		1000BaseTX	Category 5 UTP; up to 328 ft (100 m)

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
	Connector	VGA

© Copyright 2003 Hewlett-Packard Development Company, L.P.

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.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1094
Fls:
3701
Doc:

Apêndice CI

RQS Nº 03/2005 - CN
CPML - CORREIOS
Fls: 1096
Doc: 3701

TechSpecs

Integrated Smart Array 5i Plus Controller

Data Compatible with all Smart Array Controllers	Yes
Instant Upgrades to other Smart Array Controllers	Yes
Consistent Software Manageability Tools	Yes
PCI-X Bus	64-bit, 100 MHz (integrated on system board)
PCI-X Peak Data Transfer Rate	800 MB/s
SCSI Protocols Supported	Ultra3, Ultra2
SCSI Peak Data Transfer Rate	160 MB/s per channel NOTE: For ProLiant servers having TWO internal drive bays on separate SCSI ports: SCSI Peak Data Transfer Rate is 320 MB/s total; 160 MB/s per channel and Channels is 2.
Channels	2 NOTE: For ProLiant servers having two internal drive bays on separate SCSI ports: SCSI Peak Data Transfer Rate is 320 MB/s total; 160 MB/s per channel and Channels is 2.
SCSI Ports (external/internal)	0/2 NOTE: For ProLiant servers having two internal drive bays on separate SCSI ports: SCSI Peak Data Transfer Rate is 320 MB/s total; 160 MB/s per channel and Channels is 2.
Drives Supported (maximum)	Maximum = total number of drives NOTE: Maximum is the total number of internal drives on each specific ProLiant server.
Cache	64 MB Read and/or Write Cache
Battery-Backed Write Cache	Yes, with installation of Battery-Backed Write Cache Enabler, up to 64MB
RAID Support	0, 1, 1+ 0, 5
Logical Drives (maximum)	Maximum = total number of drives
Online Configuration	Yes
Online Capacity Expansion	Yes
Logical Drive Capacity Extension	Yes
Online Stripe Size Migration	Yes
Online RAID Level Migration	Yes
Online Spare Support	Yes
Automatic Data Recovery	Yes
Drive Roaming	Yes
Redundant Controllers	No

User Group Management

This chapter provides information about setting up and managing user groups in Cisco Secure Access Control Server (Cisco Secure ACS) Appliance version 3.2 to control authorization. Cisco Secure ACS enables you to group network users for more efficient administration. Each user can belong to only one group in Cisco Secure ACS. You can establish up to 500 groups to effect different levels of authorization.

Cisco Secure ACS also supports external database group mapping; that is, if your external user database distinguishes user groups, these groups can be mapped into Cisco Secure ACS. And if the external database does not support groups, you can map all users from that database to a Cisco Secure ACS user group. For information about external database mapping, see Chapter 15, "User Group Mapping and Specification".

Before you configure Group Setup, you should understand how this section functions. Cisco Secure ACS dynamically builds the Group Setup section interface depending on the configuration of your network devices and the security protocols being used. That is, what you see under Group Setup is affected by settings in the Network Configuration and Interface Configuration sections.

This chapter contains the following sections:

- **User Group Setup Features and Functions, page 6-2**—This section is an overview of the features you find within Group Setup.
- **Common User Group Settings, page 6-3**—This section details procedures that you typically would perform regardless of your particular network security configuration.

CPMI - CORREIOS
1096
3701
Fls:
3701
Doc:

- **Configuration-specific User Group Settings, page 6-15**—This section details procedures that you would perform only as applicable to your particular network security configuration.
- **Group Setting Management, page 6-52**—This section includes basic administrative procedures, such as determining the users in a group or renaming a group.

User Group Setup Features and Functions

The Group Setup section of the Cisco Secure ACS HTML interface is the centralized location for operations regarding user group configuration and administration. For information about network device groups (NDGs), see Network Device Group Configuration, page 4-36.

Default Group

If you have not configured group mapping for an external user database, Cisco Secure ACS assigns users who are authenticated by the Unknown User Policy to the Default Group the first time they log in. The privileges and restrictions for the default group are applied to first-time users. If you have upgraded from a previous version of Cisco Secure ACS and kept your database information, Cisco Secure ACS retains the group mappings you configured before upgrading.

Group TACACS+ Settings

Cisco Secure ACS enables a full range of settings for TACACS+ at the group level. If a AAA client has been configured to use TACACS+ as the security control protocol, you can configure standard service protocols, including PPP IP, PPP LCP, ARAP, SLIP, and shell (exec), to be applied for the authorization of each user who belongs to a particular group.

Note You can also configure TACACS+ settings at the user level. User-level settings always override group level settings.

ECT 14268 CPL - AC

Cisco Secure ACS also enables you to enter and configure new TACACS+ services. For information about how to configure a new TACACS+ service to appear on the group setup page, see Protocol Configuration Options for TACACS+, page 3-7.

If you have configured Cisco Secure ACS to interact with a Cisco device-management application, new TACACS+ services may appear automatically, as needed, to support the device-management application. For more information about Cisco Secure ACS interaction with device-management applications, see Support for Cisco Device-Management Applications, page 1-18.

You can use the Shell Command Authorization Set feature to configure TACACS+ group settings. This feature enables you to apply shell commands to a particular user group in the following ways:

- Assign a shell command authorization set, which you have already configured, for any network device.
- Assign a shell command authorization set, which you have already configured, to particular NDGs.
- Permit or deny specific shell commands, which you define, on a per-group basis.

For more information about shell command authorization sets, see Chapter 5, "Shared Profile Components".

Common User Group Settings

This section presents the basic activities you perform when configuring a new user group. This section contains the following procedures:

- Enabling VoIP Support for a User Group, page 6-4
- Setting Default Time-of-Day Access for a User Group, page 6-5
- Setting Callback Options for a User Group, page 6-6
- Setting Network Access Restrictions for a User Group, page 6-7
- Setting Max Sessions for a User Group, page 6-11
- Setting Usage Quotas for a User Group, page 6-13

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1097
Fls. 6-3
3701
Doc:
3701

Enabling VoIP Support for a User Group

Note If this feature does not appear, click **Interface Configuration**, click **Advanced Options**, and then select the **Voice-over-IP (VoIP) Group Settings** check box.

Perform this procedure to enable support for the null password function of VoIP. This enables users to authenticate (session or telephone call) on only the user ID (telephone number).

When you enable VoIP at the group level, all users in this group become VoIP users, and the user IDs are treated similarly to a telephone number. VoIP users do not need to enter passwords to authenticate.

Caution Enabling VoIP disables password authentication and most advanced settings, including password aging and protocol attributes.

To enable VoIP support for a group, follow these steps:

Step 1 In the navigation bar, click **Group Setup**.

Result: The Group Setup Select page opens.

Step 2 From the Group list, select the group you want to configure for VoIP support, and then click **Edit Settings**.

Result: The Group Settings page displays the name of the group at its top.

Step 3 In the Voice-over-IP Support table, select the check box labeled **This is a Voice-over-IP (VoIP) group - and all users of this group are VoIP users**.

Step 4 To save the group settings you have just made, click **Submit**.
For more information, see Saving Changes to User Group Settings, page 6-54.

Step 5 To continue, and specify other group settings, perform other procedures in this chapter, as applicable.

Setting Default Time-of-Day Access for a User Group

Note If this feature does not appear, click **Interface Configuration**, click **Advanced Options**, and then select the **Default Time-of-Day / Day-of-Week Specification** check box.

To define the times during which users in a particular group are permitted or denied access, follow these steps:

Step 1 In the navigation bar, click **Group Setup**.

Result: The Group Setup Select page opens.

Step 2 From the Group list, select a group, and then click **Edit Settings**.

Result: The Group Settings page displays the name of the group at its top.

Step 3 In the Default Time-of-Day Access Settings table, select the **Set as default Access Times** check box.

Note You must select the **Set as default Access Times** check box to limit access based on time or day.

Result: Times at which the system permits access are highlighted in green on the day and hour matrix.

Note The default sets accessibility during all hours.

Step 4 In the day and hour matrix, click the times at which you do *not* want to permit access to members of this group.

Tip Clicking times of day on the graph deselects those times; clicking again reselects them.
At any time, you can click **Clear All** to clear all hours, or you can click **Set All** to select all hours.

CPMI 6-5
1098
Fls:
Doc: 3701

Step 5 To save the group settings you have just made, click **Submit**.

For more information, see Saving Changes to User Group Settings, page 6-54.

Step 6 To continue specifying other group settings, perform other procedures in this chapter, as applicable.

Setting Callback Options for a User Group

Callback is a command string that is passed back to the access server. You can use callback strings to initiate a modem to call the user back on a specific number for added security or reversal of line charges. There are three options, as follows:

- **No callback allowed**—Disables callback for users in this group. This is the default setting.
- **Dialup client specifies callback number**—Allows the dialup client to specify the callback number. The dialup client must support RFC 1570, PPP LCP Extensions.
- **Use Windows Database callback settings (where possible)**—Uses the Microsoft Windows callback settings. If a Windows account for a user resides in a remote domain, the domain in which Cisco Secure ACS resides must have a two-way trust with that domain for the Microsoft Windows callback settings to operate for that user.

To set callback options for a user group, follow these steps:

Step 1 In the navigation bar, click **Group Setup**.

Result: The Group Setup Select page opens.

Step 2 Select a group from the Group list, and then click **Edit Settings**.

Result: The Group Settings page displays the name of the group at its top.

Step 3 In the Callback table, select one of the following three options:

- No callback allowed
- Dialup client specifies callback number
- Use Windows Database callback settings (where possible)

1426
CPL - AC

Step 4 To save the group settings you have just made, click **Submit**.

For more information, see Saving Changes to User Group Settings, page 6-54.

Step 5 To continue specifying other group settings, perform other procedures in this chapter, as applicable.

Setting Network Access Restrictions for a User Group

The Network Access Restrictions table in Group Setup enables you to apply network access restrictions (NARs) in three distinct ways:

- Apply existing shared NARs by name.
- Define IP-based group access restrictions to permit or deny access to a specified AAA client or to specified ports on a AAA client when an IP connection has been established.
- Define CLI/DNIS-based group NARs to permit or deny access to either, or both, the calling line ID (CLI) number or the Dialed Number Identification Service (DNIS) number used.

Note You can also use the CLI/DNIS-based access restrictions area to specify other values. For more information, see About Network Access Restrictions, page 5-7.

Typically, you define (shared) NARs from within the Shared Components section so that these restrictions can be applied to more than one group or user. For more information, see Shared Network Access Restrictions Configuration, page 5-9. You must have enabled the Group-Level Shared Network Access Restriction check box on the Advanced Options page of the Interface Configuration section for these options to appear in the Cisco Secure ACS HTML interface.

However, Cisco Secure ACS also enables you to define and apply a NAR for a single group from within the Group Setup section. You must have enabled the Group-Level Network Access Restriction setting under the Advanced Options page of the Interface Configuration section for single group IP-based filter options and single group CLI/DNIS-based filter options to appear in the Cisco Secure ACS HTML interface.

CRMI 6-7
1099
Fls:
3701
Doc:

Note When an authentication request is forwarded by proxy to a Cisco Secure ACS server, any NARs for TACACS+ requests are applied to the IP address of the forwarding AAA server, not to the IP address of the originating AAA client.

To set NARs for a user group, follow these steps:

Step 1 In the navigation bar, click **Group Setup**.

Result: The Group Setup Select page opens.

Step 2 From the Group list, select a group, and then click **Edit Settings**.

Result: The Group Settings page displays the name of the group at its top.

Step 3 To apply a previously configured shared NAR to this group, follow these steps:

Note To apply a shared NAR, you must have configured it under Network Access Restrictions in the Shared Profile Components section. For more information, see Shared Network Access Restrictions Configuration, page 5-9.

a. Select the **Only Allow network access when** check box.

b. To specify whether one or all shared NARs must apply for a member of the group to be permitted access, select one of the following options:

- All selected shared NARS result in permit
- Any one selected shared NAR results in permit

c. Select a shared NAR name in the Shared NAR list, and then click —> (right arrow button) to move the name into the Selected Shared NARs list.

Tip To view the server details of the shared NARs you have selected to apply, you can click either **View IP NAR** or **View CLID/DNIS NAR**, as applicable.

H.262.1

Step 4 To define and apply a NAR, for this particular user group, that permits or denies access to this group based on IP address, or IP address and port, follow these steps:

Tip You should define most NARs from within the Shared Components section so that the restrictions can be applied to more than one group or user. For more information, see Shared Network Access Restrictions Configuration, page 5-9.

a. In the Per Group Defined Network Access Restrictions section of the Network Access Restrictions table, select the **Define IP-based access restrictions** check box.

b. To specify whether the subsequent listing specifies permitted or denied IP addresses, from the Table Defines list, select either **Permitted Calling/Point of Access Locations** or **Denied Calling/Point of Access Locations**.

c. Select or enter the information in the following boxes:

- **AAA Client**—Select either All AAA Clients or the name of the NDG or the name of the individual AAA client to which to permit or deny access.
- **Port**—Type the number of the port to which to permit or deny access. You can use the wildcard asterisk (*) to permit or deny access to all ports on the selected AAA client.
- **Address**—Type the IP address or addresses to filter on when performing access restrictions. You can use the wildcard asterisk (*).

Note The total number of characters in the AAA Client list and the Port and Src IP Address boxes must not exceed 1024. Although Cisco Secure ACS accepts more than 1024 characters when you add a NAR, you cannot edit the NAR and Cisco Secure ACS cannot accurately apply it to users.

d. Click **Enter**.

Result: The specified the AAA client, port, and address information appears in the NAR Access Control list.

CPMI - CORREIOS
1100
Fls:
3701
Doc:

Step 5 To permit or deny access to this user group based on calling location or values other than an established IP address, follow these steps:

a. Select the **Define CLI/DNIS-based access restrictions** check box.

b. To specify whether the subsequent listing specifies permitted or denied values, from the Table Defines list, select one of the following:

- Permitted Calling/Point of Access Locations
- Denied Calling/Point of Access Locations

c. From the AAA Client list, select either All AAA Clients or the name of the NDG or the name of the particular AAA client to which to permit or deny access.

d. Complete the following boxes:

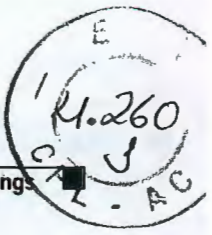
Note You must type an entry in each box. You can use the wildcard asterisk (*) for all or part of a value. The format you use must match the format of the string you receive from your AAA client. You can determine this format from your RADIUS Accounting Log.

- **PORT**—Type the number of the port to which to permit or deny access. You can use the wildcard asterisk (*) to permit or deny access to all ports.
- **CLI**—Type the CLI number to which to permit or deny access. You can use the wildcard asterisk (*) to permit or deny access based on part of the number or all numbers.

Tip This is also the selection to use if you want to restrict access based on other values, such as a Cisco Aironet client MAC address. For more information, see About Network Access Restrictions, page 5-7.

- **DNIS**—Type the DNIS number to restrict access based on the number into which the user will be dialing. You can use the wildcard asterisk (*) to permit or deny access based on part of the number or all numbers.

Tip This is also the selection to use if you want to restrict access based on other values, such as a Cisco Aironet AP MAC address. For more information, see About Network Access Restrictions, page 5-7.



Note The total number of characters in the AAA Client list and the Port, CLI, and DNIS boxes must not exceed 1024. Although Cisco Secure ACS accepts more than 1024 characters when you add a NAR, you cannot edit the NAR and Cisco Secure ACS cannot accurately apply it to users.

e. Click **Enter**.

Result: The information, specifying the AAA client, port, CLI, and DNIS appears in the list.

Step 6 To save the group settings you have just made, click **Submit**.

For more information, see Saving Changes to User Group Settings, page 6-54.

Step 7 To continue specifying other group settings, perform other procedures in this chapter, as applicable.

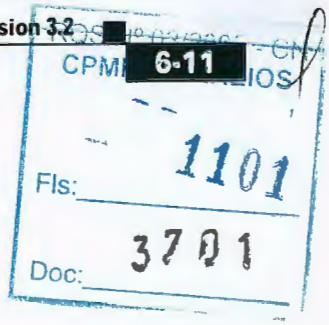
Setting Max Sessions for a User Group

Note If this feature does not appear, click **Interface Configuration**, click **Advanced Options**, and then select the **Max Sessions** check box.

Perform this procedure to define the maximum number of sessions available to a group, or to each user in a group, or both. The settings are as follows:

- **Sessions available to group**—Sets the maximum number of simultaneous connections for the entire group.
- **Sessions available to users of this group**—Sets the maximum number of total simultaneous connections for each user in this group.

Tip As an example, Sessions available to group is set to 10 and Sessions available to users of this group is set to 2. If each user is using the maximum 2 simultaneous sessions, no more than 5 users can log in.



Note A session is any type of connection supported by RADIUS or TACACS+, such as PPP, NAS prompt, Telnet, ARAP, IPX/SLIP.

Note The default setting for group Max Sessions is Unlimited for both the group and the user within the group.

To configure max sessions settings for a user group, follow these steps:

Step 1 In the navigation bar, click **Group Setup**.

Result: The Group Setup Select page opens.

Step 2 From the Group list, select a group, and then click **Edit Settings**.

Result: The Group Settings page displays the name of the group at its top.

Step 3 In the Max Sessions table, under Sessions available to group, select one of the following options:

- **Unlimited**—Select to allow this group an unlimited number of simultaneous sessions. (This effectively disables Max Sessions.)
- *n*—Type the maximum number of simultaneous sessions to allow this group.

Step 4 In the lower portion of the Max Sessions table, under Sessions available to users of this group, select one of the following two options:

- **Unlimited**—Select to allow each individual in this group an unlimited number of simultaneous sessions. (This effectively disables Max Sessions.)
- *n*—Type the maximum number of simultaneous sessions to allow each user in this group.

Note Settings made in User Setup override group settings. For more information, see Setting Max Sessions Options for a User, page 7-16.

Step 5 To save the group settings you have just made, click **Submit**.

For more information, see Saving Changes to User Group Settings, page 6-54.

ECT 14.258 SL - AC

Step 6 To continue specifying other group settings, perform other procedures in this chapter, as applicable.

Setting Usage Quotas for a User Group

Note If this feature does not appear, click **Interface Configuration**, click **Advanced Options**, and then select the **Usage Quotas** check box.

Perform this procedure to define usage quotas for members of a group. Session quotas affect each user of a group individually, not the group collectively. You can set quotas for a given period in two ways:

- By total duration of session
- By the total number of sessions

If you make no selections in the Usage Quotas section for a group, no usage quotas are enforced on users assigned to that group, unless you configure usage quotas for the individual users.

Note The Usage Quotas section on the Group Settings page does not show usage statistics.
Usage statistics are available only on the settings page for an individual user. For more information, see Setting User Usage Quotas Options, page 7-18.

When a user exceeds his or her assigned quota, Cisco Secure ACS denies that user access upon attempting to start a session. If a quota is exceeded during a session, Cisco Secure ACS allows the session to continue.

You can reset the usage quota counters for all users of a group from the Group Settings page. For more information about resetting usage quota counters for a whole group, see Resetting Usage Quota Counters for a User Group, page 6-53.

Tip To support time-based quotas, we recommend enabling accounting update packets on all AAA clients. If update packets are not enabled, the quota is updated when the user logs off. If the AAA client through which the user is accessing your

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 3701
Doc:

network fails, the quota is not updated. In the case of multiple sessions, such as with ISDN, the quota is not updated until all sessions terminate. This means that a second channel will be accepted even if the first channel has exhausted the quota for the user.

To set user usage quotas for a user group, follow these steps:

Step 1 In the navigation bar, click **Group Setup**.

Result: The Group Setup Select page opens.

Step 2 From the Group list, select a group, and then click **Edit Settings**.

Result: The Group Settings page displays the name of the group at its top.

Step 3 To define usage quotas based on duration of sessions, follow these steps:

a. In the Usage Quotas table, select the **Limit each user of this group to** *x* **hours of online time** *per time unit* check box.

b. Type the number of hours to which you want to limit group members in the **to** *x* **hours** box.
Use decimal values to indicate minutes. For example, a value of 10.5 would equal ten hours and 30 minutes.

Note Up to 5 characters are allowed in the to *x* hours box.

c. Select the period for which the quota is effective from the following:

- **per Day**—From 12:01 a.m. until midnight.
- **per Week**—From 12:01 a.m. Sunday until midnight Saturday.
- **per Month**—From 12:01 a.m. on the first of the month until midnight on the last day of the month.
- **Total**—An ongoing count of hours, with no end.

Step 4 To define user session quotas based on number of sessions, follow these steps:

a. In the Usage Quotas table, select the **Limit each user of this group to** *x* **sessions** check box.

ECT 14.256 AL - AC

b. Type the number of sessions to which you want to limit users in the **to *x* sessions** box.

Note Up to 5 characters are allowed in the to *x* sessions box.

c. Select the period for which the session quota is effective from the following:

- **per Day**—From 12:01 a.m. until midnight.
- **per Week**—From 12:01 a.m. Sunday until midnight Saturday.
- **per Month**—From 12:01 a.m. on the first of the month until midnight on the last day of the month.
- **Total**—An ongoing count of session, with no end.

Step 5 To save the group settings you have just made, click **Submit**.

For more information, see Saving Changes to User Group Settings, page 6-54.

Step 6 To continue specifying other group settings, perform other procedures in this chapter, as applicable.

Configuration-specific User Group Settings

This section details procedures that you perform only as applicable to your particular network security configuration. For instance, if you have no token server configured, you do not have to set token card settings for each group.

This section contains the following procedures:

- Setting Token Card Settings for a User Group, page 6-17
- Setting Enable Privilege Options for a User Group, page 6-18
- Enabling Password Aging for the CiscoSecure User Database, page 6-20
- Enabling Password Aging for Users in Windows Databases, page 6-25
- Setting IP Address Assignment Method for a User Group, page 6-27
- Assigning a Downloadable IP ACL to a Group, page 6-28
- Configuring TACACS+ Settings for a User Group, page 6-29

RQS Nº 03/2005 - CN - CPMI - CORREIOS
1103
Fls:
3701
Doc:

- Configuring a Shell Command Authorization Set for a User Group, page 6-31
- Configuring a PIX Command Authorization Set for a User Group, page 6-33
- Configuring Device-Management Command Authorization for a User Group, page 6-35
- Configuring IETF RADIUS Settings for a User Group, page 6-37
- Configuring Cisco IOS/PIX RADIUS Settings for a User Group, page 6-38
- Configuring Cisco Aironet RADIUS Settings for a User Group, page 6-39
- Configuring Ascend RADIUS Settings for a User Group, page 6-41
- Configuring Cisco VPN 3000 Concentrator RADIUS Settings for a User Group, page 6-42
- Configuring Cisco VPN 5000 Concentrator RADIUS Settings for a User Group, page 6-44
- Configuring Microsoft RADIUS Settings for a User Group, page 6-45
- Configuring Nortel RADIUS Settings for a User Group, page 6-47
- Configuring Juniper RADIUS Settings for a User Group, page 6-49
- Configuring BBSM RADIUS Settings for a User Group, page 6-50

Note When a vendor-specific variety of RADIUS is configured for use by network devices, the RADIUS (IETF) attributes are available because they are the base set of attributes, used as the first 74 attributes for all RADIUS vendors.

The content of these subsections is dynamic and based on two factors as follows:

- For a particular protocol to be listed, a AAA client must be configured to authenticate using that protocol. For more information, see AAA Client Configuration, page 4-11.
- The specific attributes for a particular protocol must be configured for display at the group level. For more information, see Protocol Configuration Options for TACACS+, page 3-7 or Protocol Configuration Options for RADIUS, page 3-11.

Setting Token Card Settings for a User Group

Note If this section does not appear, configure a token server. Then, click **External User Databases**, click **Database Configuration**, and then add the applicable token card server.

Perform this procedure to allow a token to be cached. This means users can use a second B channel without having to enter a second one-time password (OTP).

Caution This option is for use with token caching only for ISDN terminal adapters. You should fully understand token caching and ISDN concepts and principles before implementing this option. Token caching allows you to connect to multiple B channels without having to provide a token for each channel connection. Token card settings are applied to all users in the selected group.

Options for token caching include the following:

- **Session**—You can select Session to cache the token for the entire session. This allows the second B channel to dynamically go in and out of service.
- **Duration**—You can select Duration and specify a period of time to have the token cached (from the time of first authentication). If this time period expires, the user cannot start a second B channel.
- **Session and Duration**—You can select both Session and Duration so that, if the session runs longer than the duration value, a new token is required to open a second B channel. Type a value high enough to allow the token to be cached for the entire session. If the session runs longer than the duration value, a new token is required to open a second B channel.

To set token card settings for a user group, follow these steps:

Step 1 In the navigation bar, click **Group Setup**.

Result: The Group Setup Select page opens.

Step 2 From the Group list, select a group, and then click **Edit Settings**.

Result: The Group Settings page displays the name of the group at its top.

Step 3 From the Jump To list at the top of the page, choose **Token Cards**.

ECT 14.254 PL-AC
RQS Nº 03/2005 - CN
CPMI - CORREIOS
1104
Fls:
Doc: 3701

Step 4 In the Token Card Settings table, to cache the token for the entire session, select **Session**.

Step 5 Also in the Token Card Settings table, to cache the token for a specified time period (measured from the time of first authentication), follow these steps:

a. Select **Duration**.

b. Type the duration length in the box.

c. Select the unit of measure, either Seconds, Minutes or Hours.

Step 6 To save the group settings you have just made, click **Submit**.

For more information, see Saving Changes to User Group Settings, page 6-54.

Step 7 To continue specifying other group settings, perform other procedures in this chapter, as applicable.

Setting Enable Privilege Options for a User Group

Note If this section does not appear, click **Interface Configuration** and then click **TACACS+ (Cisco)**. At the bottom of the page in the Advanced Configuration Options table, select the **Advanced TACACS+ features** check box.

Perform this procedure to configure group-level TACACS+ enable parameters. The three possible TACACS+ enable options are as follows:

- **No Enable Privilege**—(default) Select this option to disallow enable privileges for this user group.
- **Max Privilege for Any AAA Client**—Select this option to select the maximum privilege level for this user group for any AAA client on which this group is authorized.
- **Define max Privilege on a per-network device group basis**—Select this option to define maximum privilege levels for an NDG. To use this option, you create a list of device groups and corresponding maximum privilege levels. See your AAA client documentation for information about privilege levels.

ECT 1/4.252 PL - AC

Note To define levels in this manner, you must have configured the option in Interface Configuration; if you have not done so already, click **Interface Configuration**, click **Advanced Settings**, and then select the **Network Device Groups** check box.

If you are using NDGs, this option lets you configure the NDG for enable-level mapping rather than having to do it for each user in the group.

To set enable privilege options for a user group, follow these steps:

Step 1 In the navigation bar, click **Group Setup**.

Result: The Group Setup Select page opens.

Step 2 From the Group list, select a group, and then click **Edit Settings**.

Result: The Group Settings page displays the name of the group at its top.

Step 3 From the Jump To list at the top of the page, choose **Enable Options**.

Step 4 Do one of the following:

- To disallow enable privileges for this user group, select the **No Enable Privilege** option.
- To set the maximum privilege level for this user group, for any ACS on which this group is authorized, select the **Max Privilege for Any Access Server** option. Then, select the maximum privilege level from the list.
- To define the maximum NDG privilege level for this user group, select the **Define max Privilege on a per-network device group basis** option. Then, from the lists, select the NDG and a corresponding privilege level. Finally, click **Add Association**.

  Result: The association of NDG and maximum privilege level appears in the table.

Step 5 To save the group settings you have just made, click **Submit**.

For more information, see Saving Changes to User Group Settings, page 6-54.

Step 6 To continue specifying other group settings, perform other procedures in this chapter, as applicable.

RQS N° 03/2005 - CN
CPMI - CORREIOS
1105
Fls:
Doc: 3701

Enabling Password Aging for the CiscoSecure User Database

The password aging feature of Cisco Secure ACS enables you to force users to change their passwords under one or more of the following conditions:

- After a specified number of days (age-by-date rules)
- After a specified number of logins (age-by-uses rules)
- The first time a new user logs in (password change rule)

Varieties of Password Aging Supported by Cisco Secure ACS

Cisco Secure ACS supports four distinct password aging mechanisms, as follows:

- **EAP-GTC Windows Password Aging**—Users must be in the Windows user database and be using a Microsoft client that supports EAP, such as Windows XP. For information on the requirements and configuration of this password aging mechanism, see Enabling Password Aging for Users in Windows Databases, page 6-25.
- **RADIUS-based Windows Password Aging**—Users must be in the Windows user database and be using the Windows Dial-up Networking (DUN) client. For information on the requirements and configuration of this password aging mechanism, see Enabling Password Aging for Users in Windows Databases, page 6-25.
- **Password Aging for Device-hosted Sessions**—Users must be in the CiscoSecure user database, the AAA client must be running TACACS+, and the connection must use Telnet. You can control the ability of users to change passwords during a device-hosted Telnet session. You can also control whether Cisco Secure ACS propagates passwords changed by this feature. For more information, see Local Password Management, page 8-5.
- **Password Aging for Transit Sessions**—Users must be in the CiscoSecure user database. Users must use a PPP dialup client. Further, the end-user client must have CiscoSecure Authentication Agent (CAA) installed.

Tip The CAA software is available at http://www.cisco.com.

Also, to run password aging for transit sessions, the AAA client can be running either RADIUS or TACACS+; and the AAA client must be using Cisco IOS Release 11.2.7 or later and be configured to send a watchdog accounting packet (aaa accounting new-info update) with the IP address of

ECT 1402501 CEL - AC

the calling station. (Watchdog packets are interim packets sent periodically during a session. They provide an approximate session length in the event that no stop packet is received to mark the end of the session.)

You can control whether Cisco Secure ACS propagates passwords changed by this feature. For more information, see Local Password Management, page 8-5.

Cisco Secure ACS supports password aging using the RADIUS protocol under MS CHAP versions 1 and 2. Cisco Secure ACS does not support password aging over Telnet connections using the RADIUS protocol.

Caution If a user with a RADIUS connection tries to make a Telnet connection to the AAA client during or after the password aging warning or grace period, the change password option does not appear, and the user account is expired.

Password Aging Feature Settings

This section details only the Password Aging for Device-hosted Sessions and Password Aging for Transit Sessions mechanisms. For information on the Windows Password Aging mechanism, see Enabling Password Aging for Users in Windows Databases, page 6-25. For information on configuring local password validation options, see Local Password Management, page 8-5.

The password aging feature in Cisco Secure ACS has the following options:

- **Apply age-by-date rules**—Selecting this check box configures Cisco Secure ACS to determine password aging by date. The age-by-date rules contain the following settings:
  - **Active period**—The number of days users will be allowed to log in before being prompted to change their passwords. For example, if you enter 20, users can use their passwords for 20 days without being prompted to change them. The default Active period is 20 days.
  - **Warning period**—The number of days users will be notified to change their passwords. The existing password can be used, but the Cisco Secure ACS presents a warning indicating that the password must be changed and displays the number of days left before the password expires. For example, if you enter 5 in this box and 20 in the Active period box, users will be notified to change their passwords on the 21st through 25th days.

RQS Nº 03/2005 - CN CPMI - CORREIOS 1106 Fls: 3701 Doc:

- **Grace period**—The number of days to provide as the user grace period. The grace period allows a user to log in once to change the password. The existing password can be used one last time after the number of days specified in the active and warning period fields has been exceeded. Then, a dialog box warns the user that the account will be disabled if the password is not changed, and enables the user to change it. Continuing with the examples above, if you allow a 5-day grace period, a user who did not log in during the active and warning periods would be permitted to change passwords up to and including the 30th day. However, even though the grace period is set for 5 days, a user is allowed only one attempt to change the password when the password is in the grace period. Cisco Secure ACS displays the "last chance" warning only once. If the user does not change the password, this login is still permitted, but the password expires, and the next authentication is denied. An entry is logged in the Failed-Attempts log, and the user must contact an administrator to have the account reinstated.

Note All passwords expire at midnight, not the time at which they were set.

- **Apply age-by-uses rules**—Selecting this check box configures Cisco Secure ACS to determine password aging by the number of logins. The age-by-uses rules contain the following settings:
  - **Issue warning after *x* logins**—The number of the login upon which Cisco Secure ACS begins prompting users to change their passwords. For example, if you enter 10, users are allowed to log in 10 times without a change-password prompt. On the 11th login, they are prompted to change their passwords.

Tip To allow users to log in an unlimited number of times without changing their passwords, type **-1**.

  - **Require change after *x* logins**—The number of the login after which to notify users that they must to change their passwords. Continuing with the previous example, if this number is set to 12, users receive prompts requesting them to change their passwords on their 11th and 12th login attempts. On the 13th login attempt, they receive a prompt telling them

E C T
4.248
L - AC

that they must change their passwords. If users do not change their passwords now, their accounts expire and they cannot log in. This number must be greater than the **Issue warning after *x* login** number.

Tip To allow users to log in an unlimited number of times without changing their passwords, type **-1**.

- **Apply password change rule**—Selecting this check box forces new users to change their passwords the first time they log in.
- **Generate greetings for successful logins**—Selecting this check box enables a Greetings message to display whenever users log in successfully via the CAA client. The message contains up-to-date password information specific to this user account.

The password aging rules are not mutually exclusive; a rule is applied for each check box that is selected. For example, users can be forced to change their passwords every 20 days, and every 10 logins, and to receive warnings and grace periods accordingly.

If no options are checked, passwords never expire.

Unlike most other parameters, which have corresponding settings at the user level, password aging parameters are configured only on a group basis.

Users who fail authentication because they have not changed their passwords and have exceeded their grace periods are logged in the Failed Attempts log. The accounts expire and appear in the Accounts Disabled list.

Before You Begin

- Verify that your AAA client is running the TACACS+ or RADIUS protocol. (TACACS+ only supports password aging for device-hosted sessions.)
- Set up your AAA client to perform authentication *and* accounting using the same protocol, either TACACS+ RADIUS.
- Verify that you have configured your password validation options. For more information, see Local Password Management, page 8-5.
- Set up your AAA client to use Cisco IOS Release 11.2.7 or later and to send a watchdog accounting packet (aaa accounting new-info update) with the IP address of the calling station.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1107
Fls:
Doc: 3701

To set password aging rules for a user group, follow these steps:

Step 1 In the navigation bar, click **Group Setup**.

Result: The Group Setup Select page opens.

Step 2 From the Group list, select a group, and then click **Edit Settings**.

Result: The Group Settings page displays the name of the group at its top.

Step 3 From the Jump To list at the top of the page, choose **Password Aging**.

Result: The Password Aging Rules table appears.

Step 4 To set password aging by date, select the **Apply age-by-date rules** check box and type the number of days for the following options, as applicable:

- Active period
- Warning period
- Grace period

Note Up to 5 characters are allowed in each field.

Step 5 To set password aging by use, select the **Apply age-by-uses rules** check box and type the number of logins for each of the following options, as applicable:

- Issue warning after *x* logins
- Require change after *x* logins

Note UP to 5 characters are allowed in each field.

Step 6 To force the user to change the password on the first login after an administrator has changed it, select the **Apply password change rule** check box.

Step 7 To enable a Greetings message display, select the **Generate greetings for successful logins** check box.

Step 8 To save the group settings you have just made, click **Submit**.

For more information, see Saving Changes to User Group Settings, page 6-54.

Step 9 To continue specifying other group settings, perform other procedures in this chapter, as applicable.

Enabling Password Aging for Users in Windows Databases

Cisco Secure ACS supports two types of password aging for users in Windows databases. Both types of Windows password aging mechanisms are separate and distinct from the other Cisco Secure ACS password aging mechanisms. For information on the requirements and settings for the password aging mechanisms that control users in the CiscoSecure user database, see Enabling Password Aging for the CiscoSecure User Database, page 6-20.

Note You can run both Windows Password Aging and Cisco Secure ACS Password Aging for Transit Sessions mechanisms concurrently, provided that the users authenticate from the two different databases.

The two types of password aging in Windows databases are as follows:

- **RADIUS-based password aging**—RADIUS-based password aging depends upon the RADIUS AAA protocol to send and receive the password change messages. Requirements for implementing the RADIUS-based Windows password aging mechanism include the following:
  - Communication between Cisco Secure ACS and the AAA client must be using RADIUS.
  - The AAA client must support MS CHAP password aging in addition to MS CHAP authentication.
  - Users must be in a Windows user database.
  - Users must be using the Windows DUN client.
  - You must enable MS CHAP version 1 or MS CHAP version 2, or both, in the Windows configuration within the External User Databases section.

ECT 4.246 J
ROS Nº 03/2005 - CN
CPMI - CORREIOS
1108
6-25
Fls:
3701
Doc:

Tip For information on enabling MS CHAP for password changes, see Configuring Windows Authentication, page 13-22. For information on enabling MS CHAP in System Configuration, see Global Authentication Setup, page 10-11.

- **PEAP password aging**—PEAP password aging depends upon the PEAP(EAP-GTC) or PEAP(EAP-MSCHAPv2) authentication protocol to send and receive the password change messages. Requirements for implementing the PEAP Windows password aging mechanism include the following:
  - The AAA client must support EAP.
  - Users must be in a Windows user database.
  - Users must be using a Microsoft PEAP client, such as Windows XP.
  - You must enable PEAP on the Global Authentication Configuration page within the System Configuration section.

Tip For information about enabling PEAP in System Configuration, see Global Authentication Setup, page 10-11.

  - You must enable PEAP password changes on the Windows Authentication Configuration page within the External User Databases section.

Tip For information about enabling PEAP password changes, see Configuring Windows Authentication, page 13-22.

Users whose Windows accounts reside in "remote" domains (that is, not the domain within which Cisco Secure ACS is running) can only use the Windows-based password aging if they supply their domain names.

The methods and functionality of Windows password aging differ according to which Microsoft Windows operating system you are using, and whether you employ Active Directory (AD) or Security Accounts Manager (SAM). Setting password aging for users in the Windows user database is only one part of the

ECT 4.2441 J AC

larger task of setting security policies in Windows. For comprehensive information on Windows procedures, refer to your Windows system documentation.

Setting IP Address Assignment Method for a User Group

Perform this procedure to configure the way Cisco Secure ACS assigns IP addresses to users in the group. The four possible methods are as follows:

- **No IP address assignment**—No IP address is assigned to this group.
- **Assigned by dialup client**—Use the IP address that is configured on the dialup client network settings for TCP/IP.
- **Assigned from AAA Client pool**—The IP address is assigned by an IP address pool assigned on the AAA client.
- **Assigned from AAA server pool**—The IP address is assigned by an IP address pool assigned on the AAA server.

To set an IP address assignment method for a user group, follow these steps:

Step 1 In the navigation bar, click **Group Setup**.

Result: The Group Setup Select page opens.

Step 2 From the Group list, select a group, and then click **Edit Settings**.

Result: The Group Settings page displays the name of the group at its top.

Step 3 From the Jump To list at the top of the page, choose **IP Address Assignment**.

Step 4 In the IP Assignment table, do one of the following:

- Select **No IP address assignment**.
- Select **Assigned by dialup client**.
- Select **Assigned from AAA Client pool**. Then, type the AAA client IP pool name.

ROS Nº 03/2005 - CN
CPMI - CORREIOS
1109
Fls: 6.27
Doc: 3701

- Select **Assigned from AAA pool**. Then, select the AAA server IP pool name in the Available Pools list and click —> (right arrow button) to move the name into the Selected Pools list.

Note If there is more than one pool in the Selected Pools list, the users in this group are assigned to the first available pool in the order listed.

Tip To change the position of a pool in the list, select the pool name and click **Up** or **Down** until the pool is in the position you want.

Step 5 To save the group settings you have just made, click **Submit**.

For more information, see Saving Changes to User Group Settings, page 6-54.

Step 6 To continue specifying other group settings, perform other procedures in this chapter, as applicable.

Assigning a Downloadable IP ACL to a Group

The Downloadable ACLs feature enables you to assign an IP ACL at the group level.

Note You must have established one or more IP ACLs before attempting to assign one. For instructions on how to add a downloadable IP ACL using the Shared Profile Components section of the Cisco Secure ACS HTML interface, see Adding a Downloadable IP ACL, page 5-4.

Tip The Downloadable ACLs table does not appear if it has not been enabled. To enable the Downloadable ACLs table, click **Interface Configuration**, click **Advanced Options**, and then select the **Group-Level Downloadable ACLs** check box.

To assign a downloadable IP ACL to a group, follow these steps:

Step 1 In the navigation bar, click **Group Setup**.

Result: The Group Setup Select page opens.

Step 2 From the Group list, select a group, and then click **Edit Settings**.

Result: The Group Settings page displays the name of the group at its top.

Step 3 From the Jump To list at the top of the page, choose **Downloadable ACLs**.

Step 4 Under the Downloadable ACLs section, click the **Assign IP ACL** check box.

Step 5 Select an IP ACL from the list.

Step 6 To save the group settings you have just made, click **Submit**.

For more information, see Saving Changes to User Group Settings, page 6-54.

Step 7 To continue specifying other group settings, perform other procedures in this chapter, as applicable.

Configuring TACACS+ Settings for a User Group

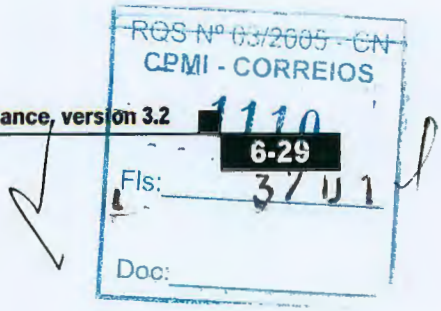
Perform this procedure to configure and enable the service/protocol parameters to be applied for the authorization of each user who belongs to the group. For information on how to configure settings for the Shell Command Authorization Set, see Configuring a Shell Command Authorization Set for a User Group, page 6-31.

Note To display or hide additional services or protocols, click **Interface Configuration**, click **TACACS+ (Cisco IOS)**, and then select or clear items in the group column, as applicable.

To configure TACACS+ settings for a user group, follow these steps:

Step 1 In the navigation bar, click **Group Setup**.

Result: The Group Setup Select page opens.



E C T
1 4.241 1
L - AC

Step 5 To allow all services to be permitted unless specifically listed and disabled, you can select the **Default (Undefined) Services** check box under the Checking this option will PERMIT all UNKNOWN Services table.

Caution This is an advanced feature and should only be used by administrators who understand the security implications.

Step 6 To save the group settings you have just made, click **Submit**.

For more information, see Saving Changes to User Group Settings, page 6-54.

Step 7 To continue specifying other group settings, perform other procedures in this chapter, as applicable.

Configuring a Shell Command Authorization Set for a User Group

Use this procedure to specify the shell command authorization set parameters for a group. There are four options:

- **None**—No authorization for shell commands.
- **Assign a Shell Command Authorization Set for any network device**—One shell command authorization set is assigned, and it applies to all network devices.
- **Assign a Shell Command Authorization Set on a per Network Device Group Basis**—Enables you to associate particular shell command authorization sets to be effective on particular NDGs.
- **Per Group Command Authorization**—Enables you to permit or deny specific Cisco IOS commands and arguments at the group level.

Note This feature requires that you have previously configured a shell command authorization set. For detailed steps, see Command Authorization Sets Configuration, page 5-19.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1111
Fls: 6.34
Doc: 3701

To specify shell command authorization set parameters for a user group, follow these steps:

Step 1 In the navigation bar, click **Group Setup**.

Result: The Group Setup Select page opens.

Step 2 From the Group list, select a group, and then click **Edit Settings**.

Result: The Group Settings page displays the name of the group at its top.

Step 3 From the Jump To list at the top of the page, choose **TACACS+**.

Result: The system displays the TACACS+ Settings table section.

Step 4 Use the vertical scrollbar to scroll to the Shell Command Authorization Set feature area.

Step 5 To prevent the application of any shell command authorization set, select (or accept the default of) the **None** option.

Step 6 To assign a particular shell command authorization set to be effective on any configured network device, follow these steps:

a. Select the **Assign a Shell Command Authorization Set for any network device** option.

b. Then, from the list directly below that option, select the shell command authorization set you want applied to this group.

Step 7 To create associations that assign a particular shell command authorization set to be effective on a particular NDG, for each association, follow these steps:

a. Select the **Assign a Shell Command Authorization Set on a per Network Device Group Basis** option.

b. Select a **Device Group** and a corresponding **Command Set**.

Tip You can select a **Command Set** that will be effective for all **Device Groups**, that are not otherwise assigned, by assigning that set to the <*default*> Device Group.

c. Click **Add Association**.

Result: The associated NDG and shell command authorization set appear in the table.

E C T
14.2391
L - A

Step 8 To define the specific Cisco IOS commands and arguments to be permitted or denied at the group level, follow these steps:

a. Select the **Per Group Command Authorization** option.

b. Under Unmatched Cisco IOS commands, select either **Permit** or **Deny**.

If you select Permit, users can issue all commands not specifically listed. If you select Deny, users can issue only those commands listed.

c. To list particular commands to be permitted or denied, select the **Command** check box and then type the name of the command, define its arguments using standard permit or deny syntax, and select whether unlisted arguments should be permitted or denied.

Caution This is a powerful, advanced feature and should be used by an administrator skilled with Cisco IOS commands. Correct syntax is the responsibility of the administrator. For information on how Cisco Secure ACS uses pattern matching in command arguments, see About Pattern Matching, page 5-19.

Tip To enter several commands, you must click **Submit** after specifying a command. A new command entry box appears below the box you just completed.

onfiguring a PIX Command Authorization Set for a User Group

Use this procedure to specify the PIX command authorization set parameters for a user group. There are three options:

- **None**—No authorization for PIX commands.
- **Assign a PIX Command Authorization Set for any network device**—One PIX command authorization set is assigned, and it applies all network devices.
- **Assign a PIX Command Authorization Set on a per Network Device Group Basis**—Particular PIX command authorization sets are to be effective on particular NDGs.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1112
Fls:
3701
Doc:

Before You Begin

- Ensure that a AAA client has been configured to use TACACS+ as the security control protocol.
- On the TACACS+ (Cisco) page of Interface Configuration section, ensure that the PIX Shell (pixShell) option is selected in the Group column.
- Make sure that you have already configured one or more PIX command authorization sets. For detailed steps, see Command Authorization Sets Configuration, page 5-19.

To specify PIX command authorization set parameters for a user group,

---

Step 1 In the navigation bar, click **Group Setup**.

Result: The Group Setup Select page opens.

Step 2 From the Group list, select a group, and then click **Edit Settings**.

Result: The Group Settings page displays the name of the group at its top.

Step 3 From the Jump To list at the top of the page, choose **TACACS+**.

Result: The system displays the TACACS+ Settings table section.

Step 4 Scroll down to the PIX Command Authorization Set feature area within the TACACS+ Settings table.

Step 5 To prevent the application of any PIX command authorization set, select (or accept the default of) the **None** option.

Step 6 To assign a particular PIX command authorization set to be effective on any configured network device, follow these steps:

a. Select the **Assign a PIX Command Authorization Set for any network device** option.

b. From the list directly below that option, select the PIX command authorization set you want applied to this user group.

Step 7 To create associations that assign a particular PIX command authorization set to be effective on a particular NDG, for each association, follow these steps:

a. Select the **Assign a PIX Command Authorization Set on a per Network Device Group Basis** option.

b. Select a **Device Group** and an associated **Command Set**.

c. Click **Add Association**.

Result: The associated NDG and PIX command authorization set appear in the table.

Note To remove or edit an existing PIX command authorization set association, you can select the association from the list, and then click **Remove Association**.

Configuring Device-Management Command Authorization for a User Group

Use this procedure to specify the device-management command authorization set parameters for a group. Device-management command authorization sets support the authorization of tasks in Cisco device-management applications that are configured to use Cisco Secure ACS for authorization. There are three options:

- **None**—No authorization is performed for commands issued in the applicable Cisco device-management application.
- **Assign a** *device-management application* for any network device—For the applicable device-management application, one command authorization set is assigned, and it applies to management tasks on all network devices.
- **Assign a** *device-management application* on a per Network Device Group Basis—For the applicable device-management application, this option enables you to apply command authorization sets to specific NDGs, so that it affects all management tasks on the network devices belonging to the NDG.

Note This feature requires that you have configured a command authorization set for the applicable Cisco device-management application. For detailed steps, see Command Authorization Sets Configuration, page 5-19.

To specify device-management application command authorization for a user group, follow these steps:

Step 1 In the navigation bar, click **Group Setup**.

Result: The Group Setup Select page opens.

Step 2 From the Group list, select a group, and then click **Edit Settings**.

Result: The Group Settings page displays the name of the group at its top.

Step 3 From the Jump To list at the top of the page, choose **TACACS+**.

Result: The system displays the TACACS+ Settings table section.

Step 4 Use the vertical scrollbar to scroll to the *device-management application* feature area, where *device-management application* is the name of the applicable Cisco device-management application.

Step 5 To prevent the application of any command authorization set for the applicable device-management application, select the **None** option.

Step 6 To assign a particular command authorization set that affects device-management application actions on any network device, follow these steps:

a. Select the **Assign a** *device-management application* for any network device option.

b. Then, from the list directly below that option, select the command authorization set you want applied to this group.

Step 7 To create associations that assign a particular command authorization set that affects device-management application actions on a particular NDG, for each association, follow these steps:

a. Select the **Assign a** *device-management application* on a per Network Device Group Basis option.

b. Select a **Device Group** and a corresponding **device-management application**.

c. Click **Add Association**.

Result: The associated NDG and command authorization set appear in the table.

E C T
4.235
J
L - AC

Configuring IETF RADIUS Settings for a User Group

These parameters appear only when both the following are true:

- A AAA client has been configured to use one of the RADIUS protocols in Network Configuration.
- Group-level RADIUS attributes have been enabled on the RADIUS (IETF) page in the Interface Configuration section of the HTML interface.

RADIUS attributes are sent as a profile for each user from Cisco Secure ACS to the requesting AAA client. To display or hide any of these attributes, see Protocol Configuration Options for RADIUS, page 3-11. For a list and explanation of RADIUS attributes, see Appendix C, "RADIUS Attributes". For more information about how your AAA client uses RADIUS, refer to your AAA client vendor documentation.

To configure IETF RADIUS attribute settings to be applied as an authorization for each user in the current group, follow these steps:

Step 1 In the navigation bar, click **Group Setup**.

Result: The Group Setup Select page opens.

Step 2 From the Group list, select a group, and then click **Edit Settings**.

Result: The Group Settings page displays the name of the group at its top.

Step 3 From the Jump To list at the top of the page, choose **RADIUS (IETF)**.

Step 4 For each IETF RADIUS attribute you need to authorize for the current group, select the check box next to the attribute and then define the authorization for the attribute in the field or fields next to it.

Step 5 To save the group settings you have just made, click **Submit**.

For more information, see Saving Changes to User Group Settings, page 6-54.

Step 6 To configure the vendor-specific attributes (VSAs) for any RADIUS network device vendor supported by Cisco Secure ACS, see the appropriate section:

- Configuring Cisco IOS/PIX RADIUS Settings for a User Group, page 6-38
- Configuring Cisco Aironet RADIUS Settings for a User Group, page 6-39
- Configuring Ascend RADIUS Settings for a User Group, page 6-41
- Configuring Cisco VPN 3000 Concentrator RADIUS Settings for a User Group, page 6-42

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1114
Fls:
3701
Doc:

- Configuring Cisco VPN 5000 Concentrator RADIUS Settings for a User Group, page 6-44
- Configuring Microsoft RADIUS Settings for a User Group, page 6-45
- Configuring Nortel RADIUS Settings for a User Group, page 6-47
- Configuring Juniper RADIUS Settings for a User Group, page 6-49
- Configuring BBSM RADIUS Settings for a User Group, page 6-50

Step 7 To continue specifying other group settings, perform other procedures in this chapter, as applicable.

Configuring Cisco IOS/PIX RADIUS Settings for a User Group

The Cisco IOS/PIX RADIUS parameters appear only when both the following are true:

- A AAA client has been configured to use RADIUS (Cisco IOS/PIX) in Network Configuration.
- Group-level RADIUS (Cisco IOS/PIX) attributes have been enabled in Interface Configuration: RADIUS (Cisco IOS/PIX).

Cisco IOS/PIX RADIUS represents only the Cisco VSAs. You must configure both the IETF RADIUS and Cisco IOS/PIX RADIUS attributes.

Note To hide or display Cisco IOS/PIX RADIUS attributes, see Setting Protocol Configuration Options for Non-IETF RADIUS Attributes, page 3-16. A VSA applied as an authorization to a particular group persists, even when you remove or replace the associated AAA client; however, if you have no AAA clients of this (vendor) type configured, the VSA settings do not appear in the group configuration interface.

ECT 4.2331 3 AC

To configure and enable Cisco IOS/PIX RADIUS attributes to be applied as an authorization for each user in the current group, follow these steps:

Step 1 Before you configure Cisco IOS/PIX RADIUS attributes, be sure your IETF RADIUS attributes are configured properly. For more information about setting IETF RADIUS attributes, see Configuring IETF RADIUS Settings for a User Group, page 6-37.

Step 2 For the Cisco attributes, determine the attributes to be authorized for the group by selecting the check box next to the attribute, and then type the commands (such as TACACS+ commands) to be packed as a RADIUS VSA.

Step 3 To save the group settings you have just made, click **Submit**.

For more information, see Saving Changes to User Group Settings, page 6-54.

Step 4 To continue specifying other group settings, perform other procedures in this chapter, as applicable.

Configuring Cisco Aironet RADIUS Settings for a User Group

The single Cisco Aironet RADIUS VSA, Cisco-Aironet-Session-Timeout, is a virtual VSA. It acts as a specialized implementation (that is, a remapping) of the IETF RADIUS Session-Timeout attribute (27) to respond to a request from a Cisco Aironet Access Point. You use it to provide a different timeout values when users in a group must be able to connect via both wireless and wired devices. This capability to provide a second timeout value specifically for WLAN connections avoids the difficulties that would arise if you had to use a standard timeout value (typically measured in hours) for a WLAN connection (that is typically measured in minutes). You do not need to use Cisco-Aironet-Session-Timeout if all members of a group will always connect only with a Cisco Aironet Access Point. Rather, use this setting when a group may connect via wired or wireless clients.

For example, imagine a user group's Cisco-Aironet-Session-Timeout set to 600 seconds (10 minutes) and that same user group's IETF RADIUS Session-Timeout set to 3 hours. When a member of this group connects via a VPN, Cisco Secure ACS uses 3 hours as the timeout value. However, if that same user connects via a Cisco Aironet Access Point, Cisco Secure ACS responds to an authentication request from the Aironet AP by sending 600 seconds in the IETF RADIUS Session-Timeout attribute. Thus, with the

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1115
Doc: 3701

Cisco-Aironet-Session-Timeout attribute configured, different session timeout values can be sent depending on whether the end-user client is a wired device or a Cisco Aironet Access Point.

The Cisco-Aironet-Session-Timeout VSA appears on the Group Setup page only when both the following are true:

- A AAA client has been configured to use RADIUS (Cisco Aironet) in Network Configuration.
- The group-level RADIUS (Cisco Aironet) attribute has been enabled in Interface Configuration: RADIUS (Cisco Aironet).

Note To hide or display the Cisco Aironet RADIUS VSA, see Setting Protocol Configuration Options for Non-IETF RADIUS Attributes, page 3-16. A VSA applied as an authorization to a particular group persists, even when you remove or replace the associated AAA client; however, if you have no AAA clients of this (vendor) type configured, the VSA settings do not appear in the group configuration interface.

To configure and enable the Cisco Aironet RADIUS attribute to be applied as an authorization for each user in the current group, follow these steps:

Step 1 Confirm that your IETF RADIUS attributes are configured properly. For more information about setting IETF RADIUS attributes, see Configuring IETF RADIUS Settings for a User Group, page 6-37.

Step 2 In the navigation bar, click **Group Setup**.

Result: The Group Setup Select page opens.

Step 3 From the Group list, select a group, and then click **Edit Settings**.

Result: The Group Settings page displays the name of the group at its top.

Step 4 From the Jump To list at the top of the page, choose **RADIUS (Cisco Aironet)**.

Step 5 In the Cisco Aironet RADIUS Attributes table, select the **[5842\001] Cisco-Aironet-Session-Timeout** check box.

E C T
14.231

Step 6 In the [5842\001] Cisco-Aironet-Session-Timeout box, type the session timeout value (in seconds) that Cisco Secure ACS is to send in the IETF RADIUS Session-Timeout (27) attribute when the AAA client is configured in Network Configuration to use the RADIUS (Cisco Aironet) authentication option. The recommended value is 600 seconds.

For more information about the IETF RADIUS Session-Timeout attribute, see Appendix C, "RADIUS Attributes" or your AAA client documentation.

Step 7 To save the group settings you have just made, click **Submit**.

For more information, see Saving Changes to User Group Settings, page 6-54.

Step 8 To continue specifying other group settings, perform other procedures in this chapter, as applicable.

Configuring Ascend RADIUS Settings for a User Group

The Ascend RADIUS parameters appear only when both the following are true:

- A AAA client has been configured to use RADIUS (Ascend) or RADIUS (Cisco IOS/PIX) in Network Configuration.
- Group-level RADIUS (Ascend) attributes have been enabled in Interface Configuration: RADIUS (Ascend).

Ascend RADIUS represents only the Ascend proprietary attributes. You must configure both the IETF RADIUS and Ascend RADIUS attributes. Proprietary attributes override IETF attributes.

The default attribute setting displayed for RADIUS is `Ascend-Remote-Addr`.

Note To hide or display Ascend RADIUS attributes, see Setting Protocol Configuration Options for Non-IETF RADIUS Attributes, page 3-16. A VSA applied as an authorization to a particular group persists, even when you remove or replace the associated AAA client; however, if you have no AAA clients of this (vendor) type configured, the VSA settings do not appear in the group configuration interface.

ROS Nº 03/2005 - CPMI
CPMI - CORREIOS
Fls: 1116
3701
Doc:

To configure and enable Ascend RADIUS attributes to be applied as an authorization for each user in the current group, follow these steps:

Step 1 Confirm that your IETF RADIUS attributes are configured properly. For more information about setting IETF RADIUS attributes, see Configuring IETF RADIUS Settings for a User Group, page 6-37.

Step 2 In the navigation bar, click **Group Setup**.

Result: The Group Setup Select page opens.

Step 3 From the Group list, select a group, and then click **Edit Settings**.

Result: The Group Settings page displays the name of the group at its top.

Step 4 From the Jump To list at the top of the page, choose **RADIUS (Ascend)**.

Step 5 In the Ascend RADIUS Attributes table, determine the attributes to be authorized for the group by selecting the check box next to the attribute. Be sure to define the authorization for that attribute in the field next to it. For more information about attributes, see Appendix C, "RADIUS Attributes" or your AAA client documentation.

Step 6 To save the group settings you have just made, click **Submit**.

For more information, see Saving Changes to User Group Settings, page 6-54.

Step 7 To continue specifying other group settings, perform other procedures in this chapter, as applicable.

Configuring Cisco VPN 3000 Concentrator RADIUS Settings for a User Group

To control Microsoft MPPE settings for users accessing the network through a Cisco VPN 3000-series concentrator, use the CVPN3000-PPTP-Encryption (VSA 20) and CVPN3000-L2TP-Encryption (VSA 21) attributes. Settings for CVPN3000-PPTP-Encryption (VSA 20) and CVPN3000-L2TP-Encryption (VSA 21) override Microsoft MPPE RADIUS settings. If either of these attributes is enabled, Cisco Secure ACS determines the values to be sent in outbound RADIUS (Microsoft) attributes and sends them along with the RADIUS (Cisco

E C T
1 4.229 1
3
L - A C

VPN 3000) attributes, regardless of whether RADIUS (Microsoft) attributes are enabled in the Cisco Secure ACS HTML interface or how those attributes might be configured.

The Cisco VPN 3000 Concentrator RADIUS attribute configurations appear only if both the following are true:

- A AAA client has been configured to use RADIUS (Cisco VPN 3000) in Network Configuration.
- Group-level RADIUS (Cisco VPN 3000) attributes have been enabled on the RADIUS (Cisco VPN 3000) page of the Interface Configuration section.

Cisco VPN 3000 Concentrator RADIUS represents only the Cisco VPN 3000 Concentrator VSA. You must configure both the IETF RADIUS and Cisco VPN 3000 Concentrator RADIUS attributes.

Note To hide or display Cisco VPN 3000 Concentrator RADIUS attributes, see Setting Protocol Configuration Options for Non-IETF RADIUS Attributes, page 3-16. A VSA applied as an authorization to a particular group persists, even when you remove or replace the associated AAA client; however, if you have no AAA clients of this (vendor) type configured, the VSA settings do not appear in the group configuration interface.

To configure and enable Cisco VPN 3000 Concentrator RADIUS attributes to be applied as an authorization for each user in the current group, follow these steps:

Step 1 Confirm that your IETF RADIUS attributes are configured properly.

For more information about setting IETF RADIUS attributes, see Configuring IETF RADIUS Settings for a User Group, page 6-37.

Step 2 In the navigation bar, click **Group Setup**.

Result: The Group Setup Select page opens.

Step 3 From the Group list, select a group, and then click **Edit Settings**.

Result: The Group Settings page displays the name of the group at its top.

Step 4 From the Jump To list at the top of the page, choose **RADIUS (Cisco VPN 3000)**.

Step 5 In the Cisco VPN 3000 Concentrator RADIUS Attributes table, determine the attributes to be authorized for the group by selecting the check box next to the attribute. Further define the authorization for that attribute in the field next to it.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1117
Doc: 3701

For more information about attributes, see Appendix C, "RADIUS Attributes", or the documentation for network devices using RADIUS.

Step 6 To save the group settings you have just made, click **Submit**.

For more information, see Saving Changes to User Group Settings, page 6-54.

Step 7 To continue specifying other group settings, perform other procedures in this chapter, as applicable.

Configuring Cisco VPN 5000 Concentrator RADIUS Settings for a User Group

The Cisco VPN 5000 Concentrator RADIUS attribute configurations display only when both the following are true:

- A network device has been configured to use RADIUS (Cisco VPN 5000) in Network Configuration.
- Group-level RADIUS (Cisco VPN 5000) attributes have been enabled on the RADIUS (Cisco VPN 5000) page of the Interface Configuration section.

Cisco VPN 5000 Concentrator RADIUS represents only the Cisco VPN 5000 Concentrator VSA. You must configure both the IETF RADIUS and Cisco VPN 5000 Concentrator RADIUS attributes.

Note To hide or display Cisco VPN 5000 Concentrator RADIUS attributes, see Setting Protocol Configuration Options for Non-IETF RADIUS Attributes, page 3-16. A VSA applied as an authorization to a particular group persists, even when you remove or replace the associated AAA client; however, if you have no AAA clients of this (vendor) type configured, the VSA settings do not appear in the group configuration interface.

E C T
4.2021
L - AC

To configure and enable Cisco VPN 5000 Concentrator RADIUS attributes to be applied as an authorization for each user in the current group, follow these steps:

Step 1 Confirm that your IETF RADIUS attributes are configured properly.

For more information about setting IETF RADIUS attributes, see Configuring IETF RADIUS Settings for a User Group, page 6-37.

Step 2 In the navigation bar, click **Group Setup**.

Result: The Group Setup Select page opens.

Step 3 From the Group list, select a group, and then click **Edit Settings**.

Result: The Group Settings page displays the name of the group at its top.

Step 4 From the Jump To list at the top of the page, choose **RADIUS (Cisco VPN 5000)**.

Step 5 In the Cisco VPN 5000 Concentrator RADIUS Attributes table, select the attributes that should be authorized for the group by selecting the check box next to the attribute. Further define the authorization for each attribute in the field next to it.

For more information about attributes, see Appendix C, "RADIUS Attributes", or the documentation for network devices using RADIUS.

Step 6 To save the group settings you have just made, click **Submit**.

For more information, see Saving Changes to User Group Settings, page 6-54.

Step 7 To continue specifying other group settings, perform other procedures in this chapter, as applicable.

Configuring Microsoft RADIUS Settings for a User Group

Microsoft RADIUS provides VSAs supporting MPPE, which is an encryption technology developed by Microsoft to encrypt PPP links. These PPP connections can be via a dial-in line, or over a VPN tunnel.

To control Microsoft MPPE settings for users accessing the network through a Cisco VPN 3000-series concentrator, use the CVPN3000-PPTP-Encryption (VSA 20) and CVPN3000-L2TP-Encryption (VSA 21) attributes. Settings for CVPN3000-PPTP-Encryption (VSA 20) and CVPN3000-L2TP-Encryption (VSA 21) override Microsoft MPPE RADIUS settings. If either of these attributes is

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1118
Doc: 3701

enabled, Cisco Secure ACS determines the values to be sent in outbound RADIUS (Microsoft) attributes and sends them along with the RADIUS (Cisco VPN 3000) attributes, regardless of whether RADIUS (Microsoft) attributes are enabled in the Cisco Secure ACS HTML interface or how those attributes might be configured.

The Microsoft RADIUS attribute configurations appear only when both the following are true:

- A network device has been configured in Network Configuration that uses a RADIUS protocol that supports the Microsoft RADIUS VSA.
- Group-level Microsoft RADIUS attributes have been enabled on the RADIUS (Microsoft) page of the Interface Configuration section.

The following Cisco Secure ACS RADIUS protocols support the Microsoft RADIUS VSA:

- Cisco IOS/PIX
- Cisco VPN 3000
- Ascend

Microsoft RADIUS represents only the Microsoft VSA. You must configure both the IETF RADIUS and Microsoft RADIUS attributes.

Note To hide or display Microsoft RADIUS attributes, see Setting Protocol Configuration Options for Non-IETF RADIUS Attributes, page 3-16. A VSA applied as an authorization to a particular group persists, even when you remove or replace the associated AAA client; however, if you have no AAA clients of this (vendor) type configured, the VSA settings do not appear in the group configuration interface.

To configure and enable Microsoft RADIUS attributes to be applied as an authorization for each user in the current group, follow these steps:

Step 1 Confirm that your IETF RADIUS attributes are configured properly.

For more information about setting IETF RADIUS attributes, see Configuring IETF RADIUS Settings for a User Group, page 6-37.

Step 2 In the navigation bar, click **Group Setup**.

Result: The Group Setup Select page opens.

E C T
Fl. 2251
CPL AC

Step 3 From the Group list, select a group, and then click **Edit Settings**.

Result: The Group Settings page displays the name of the group at its top.

Step 4 From the Jump To list at the top of the page, choose **RADIUS (Microsoft)**.

Step 5 In the Microsoft RADIUS Attributes table, specify the attributes to be authorized for the group by selecting the check box next to the attribute. Where applicable, further define the authorization for that attribute in the field next to it. For more information about attributes, see Appendix C, "RADIUS Attributes", or the documentation for network devices using RADIUS.

Note The MS-CHAP-MPPE-Keys attribute value is autogenerated by Cisco Secure ACS; there is no value to set in the HTML interface.

Step 6 To save the group settings you have just made, click **Submit**.

For more information, see Saving Changes to User Group Settings, page 6-54.

Step 7 To continue specifying other group settings, perform other procedures in this chapter, as applicable.

Configuring Nortel RADIUS Settings for a User Group

The Nortel RADIUS attribute configurations appear only when both the following are true:

- A network device has been configured in Network Configuration that uses a RADIUS protocol that supports the Nortel RADIUS VSA.
- Group-level Nortel RADIUS attributes have been enabled on the RADIUS (Nortel) page of the Interface Configuration section.

Nortel RADIUS represents only the Nortel VSA. You must configure both the IETF RADIUS and Nortel RADIUS attributes.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1119
Fls:
Doc: 3701

Note To hide or display Nortel RADIUS attributes, see Setting Protocol Configuration Options for Non-IETF RADIUS Attributes, page 3-16. A VSA applied as an authorization to a particular group persists, even when you remove or replace the associated AAA client; however, if you have no AAA clients of this (vendor) type configured, the VSA settings do not appear in the group configuration interface.

To configure and enable Nortel RADIUS attributes to be applied as an authorization for each user in the current group, follow these steps:

Step 1 Confirm that your IETF RADIUS attributes are configured properly.

For more information about setting IETF RADIUS attributes, see Configuring IETF RADIUS Settings for a User Group, page 6-37.

Step 2 In the navigation bar, click **Group Setup**.

Result: The Group Setup Select page opens.

Step 3 From the Group list, select a group, and then click **Edit Settings**.

Result: The Group Settings page displays the name of the group at its top.

Step 4 From the Jump To list at the top of the page, choose **RADIUS (Nortel)**.

Step 5 In the Nortel RADIUS Attributes table, specify the attributes to be authorized for the group by selecting the check box next to the attribute. Where applicable, further define the authorization for that attribute in the field next to it. For more information about attributes, see Appendix C, "RADIUS Attributes", or the documentation for network devices using RADIUS.

Note The MS-CHAP-MPPE-Keys attribute value is autogenerated by Cisco Secure ACS; there is no value to set in the HTML interface.

Step 6 To save the group settings you have just made, click **Submit**.

For more information, see Saving Changes to User Group Settings, page 6-54.

Step 7 To continue specifying other group settings, perform other procedures in this chapter, as applicable.

ECT 14.223 CPL - AC

Configuring Juniper RADIUS Settings for a User Group

Juniper RADIUS represents only the Juniper VSA. You must configure both the IETF RADIUS and Juniper RADIUS attributes.

Note To hide or display Juniper RADIUS attributes, see Setting Protocol Configuration Options for Non-IETF RADIUS Attributes, page 3-16. A VSA applied as an authorization to a particular group persists, even when you remove or replace the associated AAA client; however, if you have no AAA clients of this (vendor) type configured, the VSA settings do not appear in the group configuration interface.

To configure and enable Juniper RADIUS attributes to be applied as an authorization for each user in the current group, follow these steps:

Step 1 Confirm that your IETF RADIUS attributes are configured properly.

For more information about setting IETF RADIUS attributes, see Configuring IETF RADIUS Settings for a User Group, page 6-37.

Step 2 In the navigation bar, click **Group Setup**.

Result: The Group Setup Select page opens.

Step 3 From the Group list, select a group, and then click **Edit Settings**.

Result: The Group Settings page displays the name of the group at its top.

Step 4 From the Jump To list at the top of the page, choose **RADIUS (Juniper)**.

Step 5 In the Juniper RADIUS Attributes table, specify the attributes to be authorized for the group by selecting the check box next to the attribute. Where applicable, further define the authorization for that attribute in the field next to it. For more information about attributes, see Appendix C, "RADIUS Attributes", or the documentation for network devices using RADIUS.

Note The MS-CHAP-MPPE-Keys attribute value is autogenerated by Cisco Secure ACS; there is no value to set in the HTML interface.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1120
Doc: 3701

Step 6 To save the group settings you have just made, click **Submit**.

For more information, see Saving Changes to User Group Settings, page 6-54.

Step 7 To continue specifying other group settings, perform other procedures in this chapter, as applicable.

Configuring BBSM RADIUS Settings for a User Group

BBSM RADIUS represents only the BBSM RADIUS VSA. You must configure both the IETF RADIUS and BBSM RADIUS attributes.

Note To hide or display BBSM RADIUS attributes, see Setting Protocol Configuration Options for Non-IETF RADIUS Attributes, page 3-16. A VSA applied as an authorization to a particular group persists, even when you remove or replace the associated AAA client; however, if you have no AAA clients of this (vendor) type configured, the VSA settings do not appear in the group configuration interface.

To configure and enable BBSM RADIUS attributes to be applied as an authorization for each user in the current group, follow these steps:

Step 1 Confirm that your IETF RADIUS attributes are configured properly.

For more information about setting IETF RADIUS attributes, see Configuring IETF RADIUS Settings for a User Group, page 6-37.

Step 2 In the navigation bar, click **Group Setup**.

Result: The Group Setup Select page opens.

Step 3 From the Group list, select a group, and then click **Edit Settings**.

Result: The Group Settings page displays the name of the group at its top.

Step 4 From the Jump To list at the top of the page, choose **RADIUS (BBSM)**.

Step 5 In the BBSM RADIUS Attributes table, specify the attribute to be authorized for the group by selecting the check box next to the attribute. Where applicable, further define the authorization for that attribute in the field next to it. For more information about attributes, see Appendix C, "RADIUS Attributes", or the documentation for network devices using RADIUS.

Note The MS-CHAP-MPPE-Keys attribute value is autogenerated by Cisco Secure ACS; there is no value to set in the HTML interface.

Step 6 To save the group settings you have just made, click **Submit**.

For more information, see Saving Changes to User Group Settings, page 6-54.

Step 7 To continue specifying other group settings, perform other procedures in this chapter, as applicable.

Configuring Custom RADIUS VSA Settings for a User Group

User-defined, custom Radius VSA configurations appear only when all the following are true:

- You have defined and configured the custom RADIUS VSAs. (For information about creating user-defined RADIUS VSAs, see Custom RADIUS Vendors and VSAs, page 9-26.)
- A network device has been configured in Network Configuration that uses a RADIUS protocol that supports the custom VSA.
- Group-level custom RADIUS attributes have been enabled on the RADIUS (*Name*) page of the Interface Configuration section.

You must configure both the IETF RADIUS and the custom RADIUS attributes.

To configure and enable custom RADIUS attributes to be applied as an authorization for each user in the current group, follow these steps:

Step 1 Confirm that your IETF RADIUS attributes are configured properly.

For more information about setting IETF RADIUS attributes, see Configuring IETF RADIUS Settings for a User Group, page 6-37.

Step 2 In the navigation bar, click **Group Setup**.

Result: The Group Setup Select page opens.

Step 3 From the Group list, select a group, and then click **Edit Settings**.

Result: The Group Settings page displays the name of the group at its top.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 112
Doc: 3701

Step 4 From the Jump To list at the top of the page, choose **RADIUS** (*custom name*).

Step 5 In the RADIUS (*custom name*) Attributes table, specify the attributes to be authorized for the group by selecting the check box next to the attribute. Where applicable, further define the authorization for that attribute in the field next to it. For more information about attributes, see Appendix C, "RADIUS Attributes", or the documentation for network devices using RADIUS.

Note The MS-CHAP-MPPE-Keys attribute value is autogenerated by Cisco Secure ACS; there is no value to set in the HTML interface.

Step 6 To save the group settings you have just made, click **Submit**.

For more information, see Saving Changes to User Group Settings, page 6-54.

Step 7 To continue specifying other group settings, perform other procedures in this chapter, as applicable.

Group Setting Management

This section describes how to use the Group Setup section to perform a variety of managerial tasks.

This section contains the following procedures:

- Listing Users in a User Group, page 6-53
- Resetting Usage Quota Counters for a User Group, page 6-53
- Renaming a User Group, page 6-54
- Saving Changes to User Group Settings, page 6-54

E C T
4.219
J

Listing Users in a User Group

To list all users in a specified group, follow these steps:

Step 1 In the navigation bar, click **Group Setup**.

Result: The Group Setup Select page opens.

Step 2 From the Group list, select the group.

Step 3 Click **Users in Group**.

Result: The User List page for the particular group selected opens in the display area.

Step 4 To open a user account (to view, modify, or delete a user), click the name of the user in the User List.

Result: The User Setup page for the particular user account selected appears.

Resetting Usage Quota Counters for a User Group

You can reset the usage quota counters for all members of a group, either before or after a quota has been exceeded.

To reset usage quota counters for all members of a user group, follow these steps:

Step 1 In the navigation bar, click **Group Setup**.

Result: The Group Setup Select page opens.

Step 2 From the Group list, select the group.

Step 3 In the Usage Quotas section, select the **On submit reset all usage counters for all users of this group** check box.

Step 4 Click **Submit** at the bottom of the browser page.

Result: The usage quota counters for all users in the group are reset. The Group Setup Select page appears.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
FIS. 1122
Doc: 3701

Renaming a User Group

To rename a user group, follow these steps:

Step 1 In the navigation bar, click **Group Setup**.

Result: The Group Setup Select page opens.

Step 2 From the Group list, select the group.

Step 3 Click **Rename Group**.

Result: The Renaming Group: *Group Name* page appears.

Step 4 Type the new name in the **Group** field. Group names cannot contain angle brackets (< or >).

Step 5 Click **Submit**.

Note The group remains in the same position in the list. The number value of the group is still associated with this group name. Some utilities, such as the database import utility, use the numeric value associated with the group.

Result: The Select page opens with the new group name selected.

Saving Changes to User Group Settings

After you have completed configuration for a group, be sure to save your work.

To save the configuration for the current group, follow these steps:

Step 1 To save your changes and apply them later, click **Submit**. When you are ready to implement the changes, click **System Configuration**, and then click **Service Control**, and click **Restart**.

Tip To save your changes and apply them immediately, click **Submit + Restart**.

E C T
4.2171
3
C P L - A C

Result: The group attributes are applied and services are restarted. The Edit page opens.

Note Restarting the service clears the Logged-in User Report and temporarily interrupts all Cisco Secure ACS services. This affects the Max Sessions counter.

Step 2 To verify that your changes were applied, select the group and click **Edit Settings**. View the settings.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1123
Doc: 3701

Apêndice CJ

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1124
Doc:
3701

ECT
4.245
CPL - AC

Cisco Systems

Data Sheet

Cisco Intrusion Detection System 4200 Series Appliance Sensors

The Cisco Intrusion Detection System (IDS) 4200 appliance sensors are members of the market-leading Cisco IDS Series of products that provide *Pervasive Protection* throughout the network.

Introduction

The Cisco IDS 4200 Series appliance sensors are purpose-built, high-performance network security "appliances" that protect against unauthorized, malicious activity traversing the network, such as attacks by hackers. Cisco IDS sensors analyze traffic in real time, enabling users to quickly respond to security breaches.

Cisco's world-renowned Cisco Countermeasures Research Team (C-CRT) uses a combination of highly innovative and sophisticated detection techniques, including stateful pattern recognition, protocol parsing, heuristic detection, and anomaly detection, that provide comprehensive protection from a variety of both known and unknown cyber threats. Furthermore, Cisco's patent-pending Signature Micro-Engine (SME) technology allows granular customization of sensor signatures, resulting in precisely tuned sensors that minimize the occurrence of "false positives."

When unauthorized activity is detected, the sensor can send alarms to the management console(s) with details of the activity. Additionally, the Cisco IDS Active Response System delivers unparalleled protection by controlling other systems, such as routers, firewalls, and switches, to terminate unauthorized sessions. The installation and management of these turnkey appliances is easy using a wide array of management solutions, including a Web user interface, a command-line interface (CLI), or Cisco's highly scalable CiscoWorks VPN/Security Management solutions (VMS).

Application

The Cisco IDS 4200 Series of appliance sensors includes three products: the Cisco IDS 4210, the Cisco IDS 4235, and the Cisco IDS 4250. The entire Cisco IDS appliance portfolio delivers a broad range of solutions that allow easy integration into many different environments, including enterprise and service provider environments. Each appliance sensor addresses the bandwidth requirements at one of a variety of performance marks, from 45 Mbps to gigabit.

The Cisco IDS 4210 can monitor up to 45 Mbps of traffic and is suitable for T1/E1 and T3 environments.

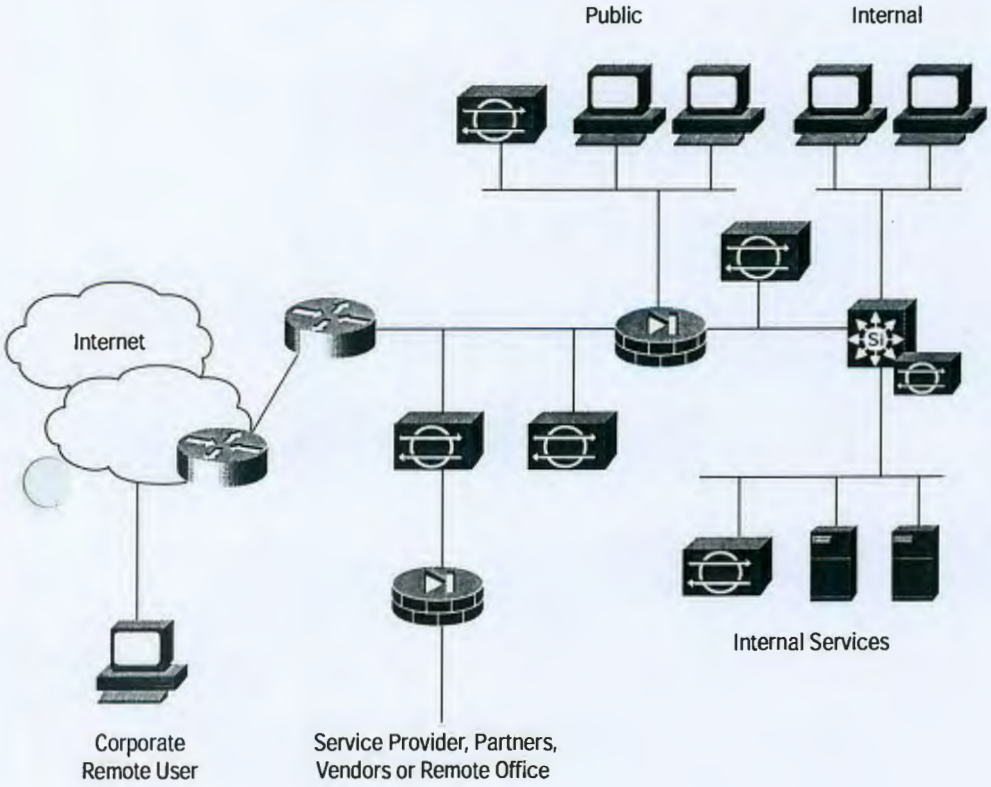
At 200 Mbps, the Cisco IDS 4235 can be deployed to provide protection in switched environments, on multiple T3 subnets, and with the support of 10/100/1000 interfaces, it can also be deployed on partially utilized gigabit links.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1125
Fls:
Doc: 3701

Cisco Systems, Inc.
All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

The Cisco IDS 4250 supports unparalleled 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.

Sensors can be placed on almost any network segment of the enterprise-wide network where security visibility is required.



Cisco Systems, Inc.
All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1126
Fls:
Doc:

E C T
4.213
J
CPL - AC

Table 1 List of characterisics of the Cisco IDS 4210, 4235, and 4250 appliance sensors.

	Cisco IDS 4210	Cisco IDS 4235	Cisco IDS 4250
Performance	45 Mbps	200 Mbps[1]	500 Mbps[2]
Standard monitoring interface	10/100BASE-T	10/100/1000BASE-TX	10/100/1000BASE-TX
Standard command and control interface	10/10 10/100BASE-T	10/100/1000BASE-TX	10/100/1000BASE-TX
Optional interface	No	No	1000BASE-SX (fiber)
Performance upgradable	No	No	Yes
Form factor	1 rack unit	1 rack unit	1 rack unit
Advanced Protection Algorithms			
Stateful pattern recognition	Yes	Yes	Yes
Protocol parsing	Yes	Yes	Yes
Heuristic detection	Yes	Yes	Yes
Anomaly detection	Yes	Yes	Yes
Attack Protection			
Sweeps/floods	Yes	Yes	Yes
DoS[1] mitigation	Yes	Yes	Yes
Worms/viruses	Yes	Yes	Yes
CGI[2]/WWW attacks	Yes	Yes	Yes
Buffer overflow protection	Yes	Yes	Yes
RPC attack detection	Yes	Yes	Yes
IP fragmentation attacks	Yes	Yes	Yes
ICMP[3] attacks	Yes	Yes	Yes
SMTP[4]/Sendmail/IMAP[5]/POP[6] attacks	Yes	Yes	Yes
FTP[7], SSH[8], Telnet, and rlogin attacks	Yes	Yes	Yes
DNS[9] attacks	Yes	Yes	Yes
TCP hijacks	Yes	Yes	Yes
Windows/NetBIOS attacks	Yes	Yes	Yes

RQS Nº 03/2005 - CN
CPMI CORREIOS
1127
Fls:
Doc: 3701

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

	Cisco IDS 4210	Cisco IDS 4235	Cisco IDS 4250
TCP application protection	Yes	Yes	Yes
BackOrifice attacks	Yes	Yes	Yes
NTP[10] attacks	Yes	Yes	Yes
Customizable signatures using SME technology	Yes	Yes	Yes
Automated signature updates	Yes	Yes	Yes
Alarm summarization	Yes	Yes	Yes
Support for 802.1q traffic	Yes	Yes	Yes
Secure Communication			
IPSec[11]/SSL[12] between sensor and management console	Yes	Yes	Yes
Encrypted signature packages	Yes	Yes	Yes
SSH for remote administration	Yes	Yes	Yes
SC[13] support for secure file tr[illegible]er	Yes	Yes	Yes
IDS Evasion Protection			
IP fragmentation reassembly	Yes	Yes	Yes
TCP stream reassembly	Yes	Yes	Yes
Unicode deobfuscation	Yes	Yes	Yes
Active Response Actions			
Router ACL[14] modifications	Yes	Yes	Yes
Firewall policy modifications	Yes	Yes	Yes
Switch ACL modifications	Yes	Yes	Yes
Session termination via TCP resets	Yes	Yes	Yes
IP session logging/session replay	Yes	Yes	Yes
Active Notification Actions			
Alarm display	Yes	Yes	Yes
E-[illegible] alerts	Yes	Yes	Yes
E-page alerts	Yes	Yes	Yes
Customizable script execution	Yes	Yes	Yes
Multiple alarm destinations	Yes	Yes	Yes
Third-party tool integration	Yes	Yes	Yes
IDS active update bulletins	Yes	Yes	Yes
Administration			
Web user interface (HTTPS[15])	Yes	Yes	Yes
CLI (console)	Yes	Yes	Yes

Cisco Systems, Inc.
All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1128
Doc: 3701

	Cisco IDS 4210	Cisco IDS 4235	Cisco IDS 4250
CLI (Telnet/SSH)	Yes	Yes	Yes
Cisco VMS support	Yes	Yes	Yes
High Availability			
Redundant power supply	No	Yes	Yes
Failure Detection			
Monitoring link failure detection	Yes	Yes	Yes
Communications failure detection	Yes	Yes	Yes
Services failure detection	Yes	Yes	Yes
Device failure detection	Yes	Yes	Yes
Dimensions			
Height	1.7 in. (4.32 cm)	1.67 in. (4.24 cm)	1.67 in. (4.24 cm)
Width	16.8 in. (42.54 cm)	17.6 in. (44.70 cm)	17.6 in. (44.70 cm)
[illegible]h	22 in. (55.8 cm)	27.0 in. (68.58 cm)	27.0 in. (68.58 cm)
Weight	23 lb (10.43 kg)	35 lb (15.88 kg)	35 lb (15.88 kg)
Rack-mountable	Yes	Yes	Yes
Power			
Autoswitching	100–240 VAC	110–220 VAC	110–220 VAC
Frequency	50–60 Hz	50–60 Hz	50–60 Hz
Operating current	2.0A at 115V 1.0A at 220V	2.7A at 115V 1.3A at 220V	2.7A at 115V 1.3A at 220V
Operating Environment			
Operating temperature	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	–40° to 70°C (–40° to 158°F)	–40° to 65°C (–40° to 149°F)	–40° to 65°C (–40° to 149°F)
Operating relative humidity	8 to 80% at 30°C (noncondensing)	8 to 80% (noncondensing)	8 to 80% (noncondensing)
Nonoperating relative humidity	5 to 95% (noncondensing)	5 to 95% (noncondensing)	5 to 95% (noncondensing)
Heat dissipation (worst case with [illegible]ower usage)	898 Btu/hr (maximum)	983 Btu/hr (maximum)	983 Btu/hr (maximum)

[1]Denial of service
[2]Common Gateway Interface
[3]Internet Control Message Protocol
[4]Simple Mail Transfer Protocol
[5]Internet Message Access Protocol
[6]Post Office Protocol
[7]File Transfer Protocol
[8]Secure Shell Protocol
[9]Domain Name System
[10]Network Timing Protocol
[11]IP Security
[12]Secure Sockets Layer
[13]Serial Control Protocol
[14]Access control list
[15]HTTP Secure

Cisco Systems, Inc.
All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

PROS Nº 03/2005 - CN
CPMI - CORREIOS
1129
Fls:
3701
Doc:

Note:

- 1 200 Mbps performance for IDS 4235 is based on the following conditions: 2200 new TCP connections per second, 2200 HTTP Transactions per second, Average Packet Size 438 Bytes
- 2 500 Mbps performance for IDS 4250 is based on the following conditions: 2700 new TCP connections per second, 2700 HTTP Transactions per second, Average Packet Size 456 Bytes

Agency Approvals

- *Emissions:* 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 Mark
- *Safety:* UL 1950, CSA 22.2 No.950, IEC 60950, EN 60950, AS/NZS 3260, CE Mark

Table 2 Ordering Information for Cisco IDS 4200 Series Appliance Sensor

Product number	Product description
IDS-4210-K9	Cisco IDS 45 Mbps Appliance Sensor (chassis, software, SSH, 10/100BASE-T with RJ-45 connector)
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)
ID[illegible]0-SX-INT=	1000BASE-SX monitoring interface with SC connector
IDS-PWR=	Spare power supply for the Cisco IDS 4235/4250 appliance sensors
IDS-SCSI=	Spare SCSI[1] hard disk drive for Cisco IDS 4250 Appliance Sensor
IDS-RAIL-2=	Two post rail kits for the Cisco IDS 4235/4250 Sensor platforms
IDS-RAIL-4=	Four post rail kits for the Cisco IDS 4235/4250 Sensor platforms
CON-SNT-IDS4210	Cisco SMARTnet™ 8 x 5 x NBD[2] service (Cisco IDS 4210)
CON-SNTE-IDS4210	Cisco SMARTnet 8 x 5 x 4 enhanced service (Cisco IDS 4210)
CON-SNTP-IDS4210	Cisco SMARTnet 24 x 7 x 4 premium service (Cisco IDS 4210)
CON-OS-IDS4210	Cisco SMARTnet 8 x 5 x NBD Onsite standard service Cisco (IDS 4210)
CON-OSE-IDS4210	Cisco SMARTnet 8 x 5 x 4 Onsite enhanced service (Cisco IDS 4210)
CON-OSP-IDS4210	Cisco SMARTnet 24 x 7 x 4 Onsite premium service (Cisco IDS 4210)
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)
C[illegible]NT-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	SMARTnet Onsite support 8 x 5 x 4 (Cisco IDS 4250-SX)
CON-OSP-IDS4250SK	SMARTnet Onsite support 24 x 7 x 4 (Cisco IDS 4250-SX)

[1]Small Computer Serial Interface [2]Next business day

Cisco Systems, Inc.
All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1130
Doc: 3701

4.209
J

Export Considerations

The Cisco IDS 4200 Series appliance sensors are subject to export controls. Refer to the export compliance Web site for guidance at:

htt://www.cisco.com/wwl/export/crypto/

For specific export questions, contact export@cisco.com.

Additional Information

Cisco Intrusion Detection System:

http://www.cisco.com/go/ids

Cisco VMS Solutions (IDS Management):

http://www.cisco.com/go/vms

NETWORK NEWS EDITOR'S CHOICE

NSS tested

CHANNEL CHAMPIONS 2002 INTRUSION DETECTION

INDEPENDENT LAB TESTED NETWORKS AS ADVERTISED™ MIER COMMUNICATIONS, INC.

Recommended

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

Copyright © 2002, Cisco Systems, Inc. All rights reserved. Cisco, Cisco Systems, Cisco IOS, and the Cisco Systems logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries. All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0203R)

ECT 43/2002 CN
CPMI - CORREIOS
Fls: 1131
3701
Doc:

Apêndice CL

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1132
Doc: 3701

4.164

Step 7 Select one or more of the **Action** check boxes to specify the actions that you want the sensor to take when detecting a particular attack:

Note Setting actions does not determine whether or not an alarm is logged or sent to an additional destination. See the "Configuring Event Logging" section on page 88 and/or "Adding Remote Hosts" section on page 24 for more information.

- Block—The sensor issues a command to a PIX Firewall or Cisco router. That device then denies the host or network from which the attack originated entry to the monitored network.
- IP Log—The sensor generates an IP session log with information about the attack. An IP session log contains binary data for all packets to and from the source address of the alarm.

Caution Generation of IP logs slows down the performance of the sensor. Use only when necessary.

Caution You do not have to set the action to IP Log to log the alarm. You only need the IP Log action if you want to log the binary packets to an IP log file.

- TCP Reset—The sensor resets the TPC session in which the attack signature was detected.

Note For the alarm to take no actions for that signature, deselect all the check boxes. Some actions are not available for each signature.

Step 8 Add any appropriate comments in the Comments field.

Step 9 In the Signature Name field, enter the signature name.

Step 10 Enter the values for the remaining parameters.

Note You must enter values for the parameters that are required. The other parameters are optional.

Refer to *Cisco Intrusion Detection System Signature Engines Version 3.1* found at the following website for more information on parameter values:

http://www.cisco.com/univercd/cc/td/doc/product/iaabu/csids/csids8/index.htm

Note To reset the form, click **Reset**.

Step 11 Click **OK**.

Result: The custom signature now appears in the Custom Signatures section.

Step 12 To delete the signature that you just created, select the check box, and then click **Delete**.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1133
Fls: 45
Doc: 3701

TCP Connection Signatures

TCP connection signatures are user-configurable signatures based on the transport-layer protocol (TCP) and the port number of the packets being monitored. You can enable/disable signatures, change the severity level or action associated with a signature, and add new TCP connection signatures.

Note The level of traffic logging determines the type of packets that fire TCP connection signatures. By default, only TCP connection requests (SYN packets) fire the alarm. See the "Configuring the Level of Traffic Logging" section on page 74 for more information.

This section includes these topics:

- Configuring TCP Connection Signatures, page 46
- Adding TCP Connection Signatures, page 49

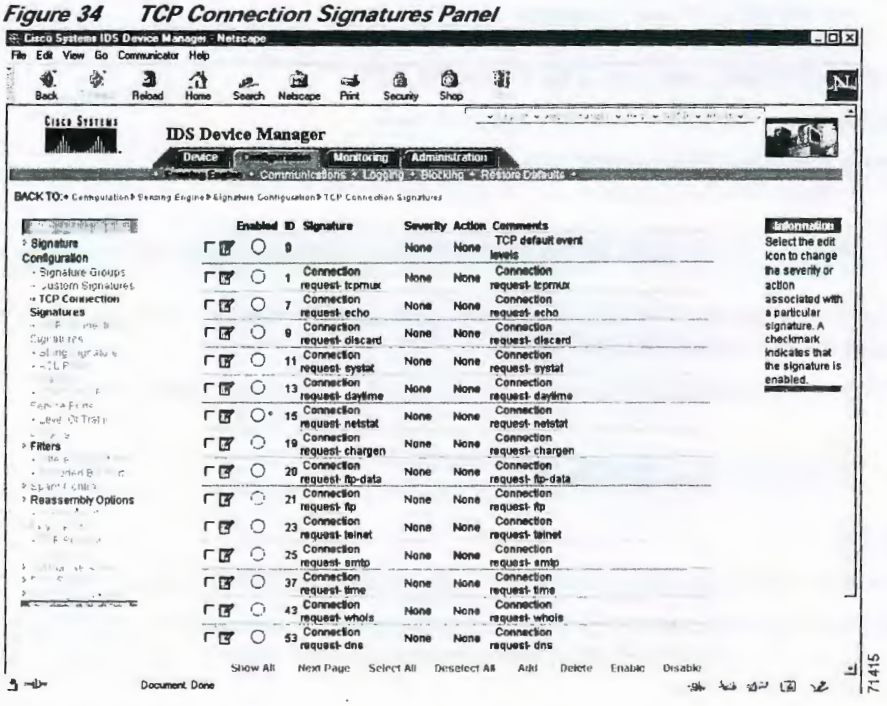
Configuring TCP Connection Signatures

To configure TCP connection signatures, follow these steps:

Step 1 In the IDS Device Manager main window, select **Configuration > Sensing Engine > TCP Connection Signatures**.

Result: The TCP Connection Signatures panel appears.

Figure 34 TCP Connection Signatures Panel



Step 2 Select the signature(s) check box that you want to enable, and then click **Enable**.

Result: The circle is now solid indicating that the signature is enabled.

E C
4.162
1
L - AG

Note Enabling a signature sets the severity for that signature to its default severity level.

Note Show All displays the entire list of TCP connection signatures. Next Page allows you to page through the entire list of TCP connection signatures. The Go to Page list box allows you to page through the entire list of TCP connection signatures by selecting a page in the list box, and then clicking Go to Page. See the "Setting Signature Pagination" section on page 126 for the procedure for setting IDS Device Manager signature pagination.

Step 3 Select the signature(s) check box that you want to disable, and then click **Disable**.

Result: The circle is now clear indicating that the signature is disabled.

Note Disabling a signature sets the severity level for that signature to None.

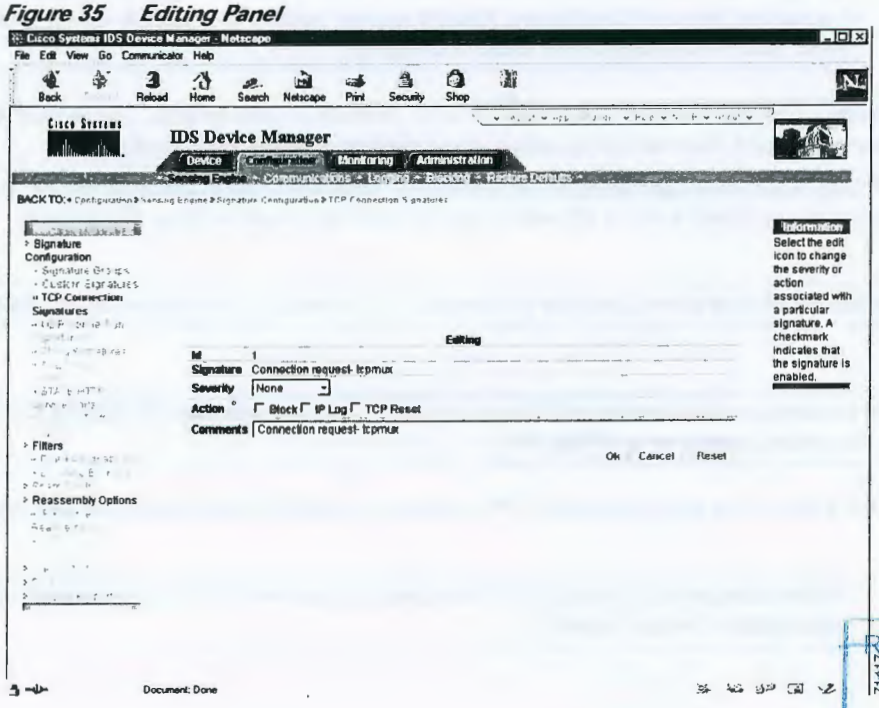
Step 4 Select the signature(s) check box that you want to delete, and then click **Delete**.

Result: The signature has disappeared from the list.

Step 5 Click the edit icon to change the severity level or action for a TCP connection signature.

Result: The Editing panel appears.

Figure 35 Editing Panel



RQS Nº 03/2005 - CN - CPMI - CORREIOS
1134
Fls:
3701
Doc:

3701

Step 6 From the Severity list box, select the severity level of the signature:

- None

Note Selecting any value other than None automatically enables the signature. Selecting None disables the signature. If you chose None at this point and want to enable the signature later, you can do so by editing the Severity level again or enabling the signature through the Signature Groups panel. See "Enabling/Disabling/Editing Signatures Within a Group List" section on page 33 for more information.

- Information—Categorizes the attack as not relevant to security. These attacks are shown with a blue icon in the IDS Event Viewer.
- Low—Categorizes the attack as mildly severe. These attacks are shown with a yellow icon in the IDS Event Viewer.
- Medium—Categorizes the attack as moderately sever. These attacks are shown with a orange icon in the IDS Event Viewer.
- High—Categorizes the attack as highly severe. These attacks are shown with a red icon in the IDS Event Viewer.

Step 7 Select one or more of the **Action** check boxes to specify the actions that you want the sensor to take when detecting a particular attack:

Note Setting actions does not determine whether or not an alarm is logged or sent to an additional destination. See the "Configuring Event Logging" section on page 88 and/or "Adding Remote Hosts" section on page 24 for more information.

- Block—The sensor issues a command to a PIX Firewall or Cisco router. That device then denies the host or network from which the attack originated entry to the monitored network.
- IP Log—The sensor generates an IP session log with information about the attack. An IP session log contains binary data for all packets to and from the source address of the alarm.

Caution Generation of IP logs slows down the performance of the sensor. Use only when necessary.

Caution You do not have to set the action to IP Log to log the alarm. You only need the IP Log action if you want to log the binary packets to an IP log file.

- TCP Reset—The sensor resets the TPC session in which the attack signature was detected.

Note For the alarm to take no actions for that signature, deselect all the check boxes. Some actions are not available for each signature.

4.160
3

Step 8 Add any appropriate comments in the Comments field.

Note To reset the form, click **Reset**.

Step 9 Click **OK**.

Adding TCP Connection Signatures

To add TCP connection signatures, follow these steps:

Step 1 In the IDS Device Manager main window, select **Configuration > Sensing Engine > TCP Connection Signatures**.

Result: The TCP Connection Signatures panel appears.

Figure 36 TCP Connection Signatures Panel

Step 2 Click **Add** to add a new TCP connection signature.

Result: The Adding panel appears.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1135
Fls:
3701
Doc:

F
1 4.359
CPL J

Figure 37 Adding Panel

Step 3 Enter the ID number for the new signature.

Value: (1–65535)

Step 4 From the Severity list box, select one of the following to change the severity level of a signature:

- None

Note Selecting any value other than None automatically enables the signature. Selecting None disables the signature. If you chose None at this point and want to enable the signature later, you can do so by editing the Severity level again or enabling the signature through the Signature Groups panel. See "Enabling/Disabling/Editing Signatures Within a Group List" section on page 33 for more information.

- Information—Categorizes the attack as not relevant to security. These attacks are shown with a blue icon in the IDS Event Viewer.
- Low—Categorizes the attack as mildly severe. These attacks are shown with a yellow icon in the IDS Event Viewer.
- Medium—Categorizes the attack as moderately sever. These attacks are shown with a orange icon in the IDS Event Viewer.
- High—Categorizes the attack as highly severe. These attacks are shown with a red icon in the IDS Event Viewer.

4.158

Step 5 Select one or more of the **Action** check boxes to specify the actions that you want the sensor to take when detecting a particular attack:

Note Setting actions does not determine whether or not an alarm is logged or sent to an additional destination. See the "Configuring Event Logging" section on page 88 and/or "Adding Remote Hosts" section on page 24 for more information.

- Block—The sensor issues a command to a PIX Firewall or Cisco router. That device then denies the host or network from which the attack originated entry to the monitored network.
- IP Log—The sensor generates an IP session log with information about the attack. An IP session log contains binary data for all packets to and from the source address of the alarm.

Caution Generation of IP logs slows down the performance of the sensor. Use only when necessary.

Caution You do not have to set the action to IP Log to log the alarm. You only need the IP Log action if you want to log the binary packets to an IP log file.

- TCP Reset—The sensor resets the TPC session in which the attack signature was detected.

Note For the alarm to take no actions for that signature, deselect all the check boxes. Some actions are not available for each signature.

Step 6 Add any appropriate comments in the Comments field.

Note Add a name for the new TCP connection signature in the Comments field.

Note To reset the form, click **Reset**.

Step 7 Click **OK**.

Step 8 To enable the TCP connection signature that you just added, find the new signature in the list of TCP signatures, select the check box, and then click **Enable**.

UDP Connection Signatures

UDP Connection Signatures are user-configurable signatures based on the transport-layer protocol (UDP) and port number of the packets being monitored. You can enable/disable signatures, change the severity level or action associated with a signature, and add new UDP connection signatures.

Note The level of traffic logging determines the type of packets that fire UDP connection signatures. By default, only UDP connection requests (SYN packets) fire the alarm. See the "Configuring the Level of Traffic Logging" section on page 74 for more information.

ROS Nº 03/2005 - CN
CPMI - CORREIOS
1136
Fls:
Doc: 3701

This section includes these topics:

- Configuring UDP Connection Signatures, page 52
- Adding UDP Connection Signatures, page 54

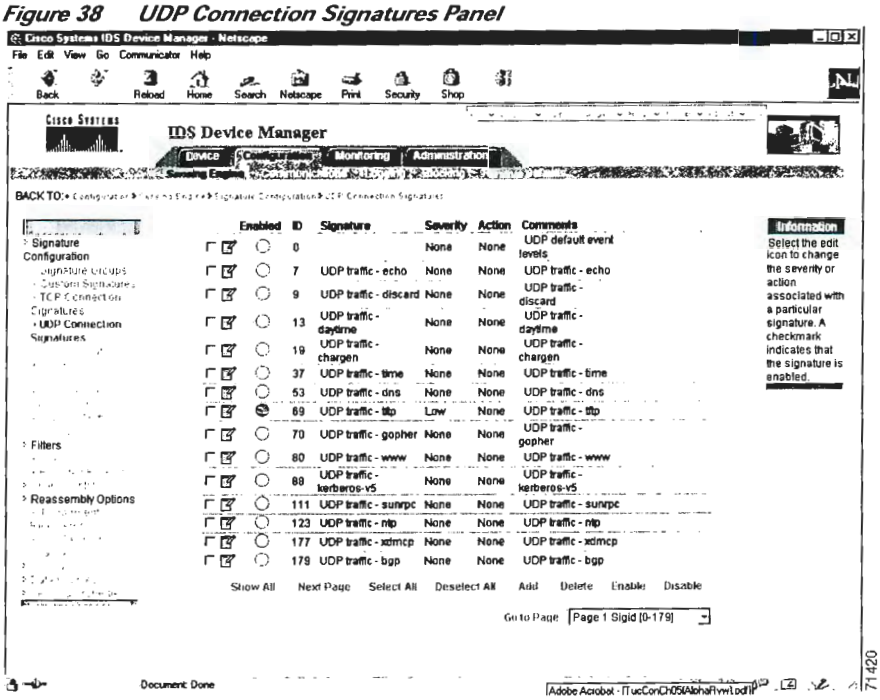
Configuring UDP Connection Signatures

To configure UDP connection signatures, follow these steps:

Step 1 In the IDS Device Manager main window, select **Configuration > Sensing Engine > UDP Connection Signatures**.

Result: The UDP Connection Signatures panel appears.

Figure 38 UDP Connection Signatures Panel



Step 2 Select the signature(s) check box that you want to enable, and then click **Enable**.

Result: The circle is now solid indicating that the signature is enabled.

Note Enabling a signature sets the severity for that signature to its default severity level.

Note Show All displays the entire list of UDP connection signatures. Next Page allows you to page through the entire list of UDP connection signatures. The Go to Page list box allows you to page through the entire list of UDP connection signatures by selecting a page in the list box, and then clicking Go to Page. See the "Setting Signature Pagination" section on page 126 for the procedure for setting IDS Device Manager signature pagination.

4.160

Step 8 Add any appropriate comments in the Comments field.

Note To reset the form, click **Reset**.

Step 9 Click **OK**.

Adding TCP Connection Signatures

To add TCP connection signatures, follow these steps:

Step 1 In the IDS Device Manager main window, select **Configuration > Sensing Engine > TCP Connection Signatures**.

Result: The TCP Connection Signatures panel appears.

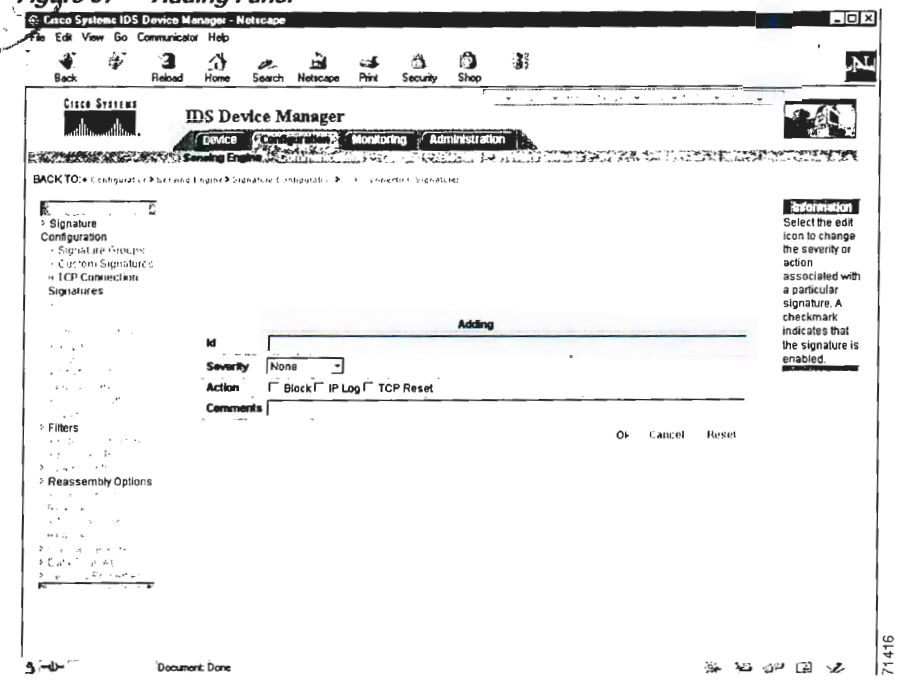
Figure 36 TCP Connection Signatures Panel

Step 2 Click **Add** to add a new TCP connection signature.

Result: The Adding panel appears.

RQS Nº 03/2005 - CN - CPMI - CORREIOS
1137
Fls:
Doc: 3701

Figure 37 Adding Panel



Step 3 Enter the ID number for the new signature.

Value: (1–65535)

Step 4 From the Severity list box, select one of the following to change the severity level of a signature:

- None

Note Selecting any value other than None automatically enables the signature. Selecting None disables the signature. If you chose None at this point and want to enable the signature later, you can do so by editing the Severity level again or enabling the signature through the Signature Groups panel. See "Enabling/Disabling/Editing Signatures Within a Group List" section on page 33 for more information.

- Information—Categorizes the attack as not relevant to security. These attacks are shown with a blue icon in the IDS Event Viewer.
- Low—Categorizes the attack as mildly severe. These attacks are shown with a yellow icon in the IDS Event Viewer.
- Medium—Categorizes the attack as moderately sever. These attacks are shown with a orange icon in the IDS Event Viewer.
- High—Categorizes the attack as highly severe. These attacks are shown with a red icon in the IDS Event Viewer.

4.158

Step 5 Select one or more of the **Action** check boxes to specify the actions that you want the sensor to take when detecting a particular attack:

Note Setting actions does not determine whether or not an alarm is logged or sent to an additional destination. See the "Configuring Event Logging" section on page 88 and/or "Adding Remote Hosts" section on page 24 for more information.

- Block—The sensor issues a command to a PIX Firewall or Cisco router. That device then denies the host or network from which the attack originated entry to the monitored network.
- IP Log—The sensor generates an IP session log with information about the attack. An IP session log contains binary data for all packets to and from the source address of the alarm.

Caution Generation of IP logs slows down the performance of the sensor. Use only when necessary.

Caution You do not have to set the action to IP Log to log the alarm. You only need the IP Log action if you want to log the binary packets to an IP log file.

- TCP Reset—The sensor resets the TPC session in which the attack signature was detected.

Note For the alarm to take no actions for that signature, deselect all the check boxes. Some actions are not available for each signature.

Step 6 Add any appropriate comments in the Comments field.

Note Add a name for the new TCP connection signature in the Comments field.

Note To reset the form, click **Reset**.

Step 7 Click **OK**.

Step 8 To enable the TCP connection signature that you just added, find the new signature in the list of TCP signatures, select the check box, and then click **Enable**.

UDP Connection Signatures

UDP Connection Signatures are user-configurable signatures based on the transport-layer protocol (UDP) and port number of the packets being monitored. You can enable/disable signatures, change the severity level or action associated with a signature, and add new UDP connection signatures.

Note The level of traffic logging determines the type of packets that fire UDP connection signatures. By default, only UDP connection requests (SYN packets) fire the alarm. See the "Configuring the Level of Traffic Logging" section on page 74 for more information.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1138
Doc: 3701

This section includes these topics:

- Configuring UDP Connection Signatures, page 52
- Adding UDP Connection Signatures, page 54

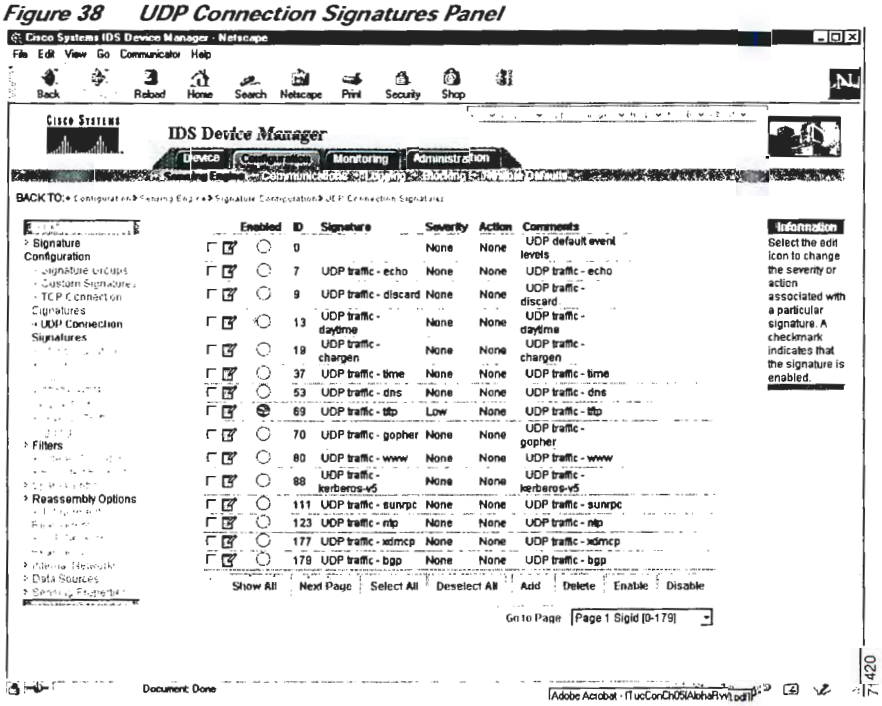
Configuring UDP Connection Signatures

To configure UDP connection signatures, follow these steps:

Step 1 In the IDS Device Manager main window, select **Configuration > Sensing Engine > UDP Connection Signatures**.

Result: The UDP Connection Signatures panel appears.

Figure 38 UDP Connection Signatures Panel



Step 2 Select the signature(s) check box that you want to enable, and then click **Enable**.

Result: The circle is now solid indicating that the signature is enabled.

Note Enabling a signature sets the severity for that signature to its default severity level.

Note Show All displays the entire list of UDP connection signatures. Next Page allows you to page through the entire list of UDP connection signatures. The Go to Page list box allows you to page through the entire list of UDP connection signatures by selecting a page in the list box, and then clicking Go to Page. See the "Setting Signature Pagination" section on page 126 for the procedure for setting IDS Device Manager signature pagination.

24.156

Step 3 Select the signature(s) check box that you want to disable, and then click **Disable**.

Result: The circle is now clear indicating that the signature is disabled. .

Note Disabling a signature sets the severity level for that signature to None.

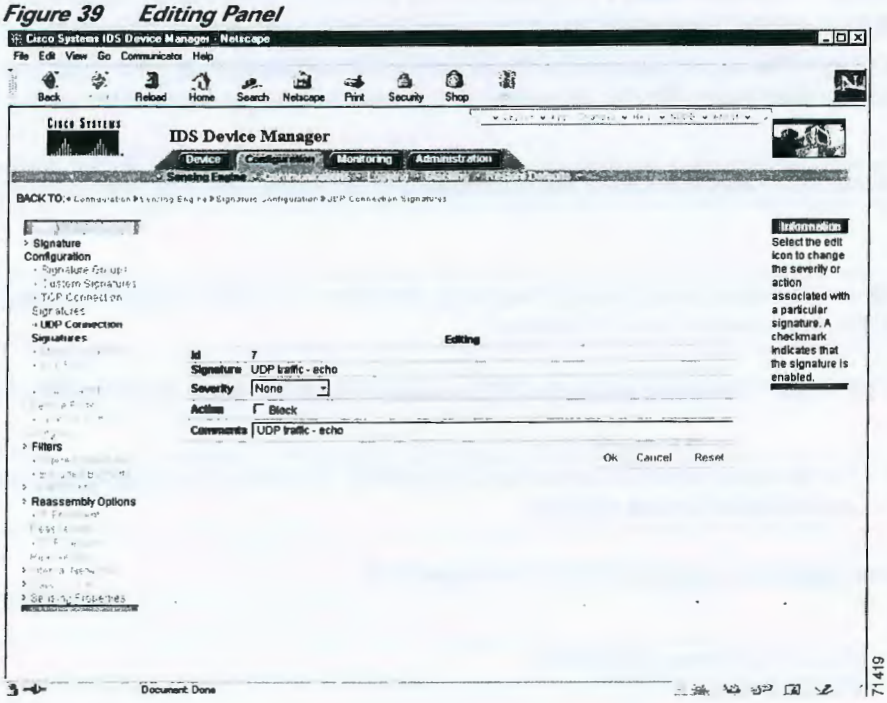
Step 4 Select the signature(s) check box that you want to delete, and then click **Delete**.

Result: The signature has disappeared from the list.

Step 5 Click the edit icon to change the severity level or action for a UDP connection signature.

Result: The Editing panel appears.

Figure 39 Editing Panel



Step 6 From the Severity list box, select the severity level of the signature:

- None

Note Selecting any value other than None automatically enables the signature. Selecting None disables the signature. If you chose None at this point and want to enable the signature later, you can do so by editing the Severity level again or enabling the signature through the Signature Groups panel. See "Enabling/Disabling/Editing Signatures Within a Group List" section on page 33 for more information.

- Information—Categorizes the attack as not relevant to security. These attacks are shown with a blue icon in the IDS Event Viewer.
- Low—Categorizes the attack as mildly severe. These attacks are shown with a yellow icon in the IDS Event Viewer.

ROS Nº 03/2005 - CN
CPMI - CORREIOS
1139
Fls.:
3701
Doc:

Medium—Categorizes the attack as moderately sever. These attacks are shown with a orange icon in the IDS Event Viewer.

- High—Categorizes the attack as highly severe. These attacks are shown with a red icon in the IDS Event Viewer.

Step 7 Select one or more of the **Action** check boxes to specify the actions that you want the sensor to take when detecting a particular attack:

Note Setting actions does not determine whether or not an alarm is logged or sent to an additional destination. See the "Configuring Event Logging" section on page 88 and/or "Adding Remote Hosts" section on page 24 for more information.

- Block—The sensor issues a command to a PIX Firewall or Cisco router. That device then denies the host or network from which the attack originated entry to the monitored network.
- IP Log—The sensor generates an IP session log with information about the attack. An IP session log contains binary data for all packets to and from the source address of the alarm.

Caution Generation of IP logs slows down the performance of the sensor. Use only when necessary.

Caution You do not have to set the action to IP Log to log the alarm. You only need the IP Log action if you want to log the binary packets to an IP log file.

- TCP Reset—The sensor resets the TPC session in which the attack signature was detected.

Note For the alarm to take no actions for that signature, deselect all the check boxes. Some actions are not available for each signature.

Step 8 Add any appropriate comments in the Comments field.

Note To reset the form, click **Reset**.

Click **OK**.

Adding UDP Connection Signatures

To add UDP connection signatures, follow these steps:

Step 1 In the IDS Device Manager main window, select **Configuration > Sensing Engine > UDP Connection Signatures**.

Result: The UDP Connection Signatures panel appears.

4.154
CPL

Figure 40 UDP Connection Signatures Panel

Step 2 Click **Add** to add a new UDP connection signature.

Result: The Adding panel appears.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1140
Fls:
3701
Doc:

Figure 41 Adding Panel

Step 3 Enter the ID number for the new signature.

Value: (1–65535)

Step 4 From the Severity list box, select the severity level of the signature:

- None

Note Selecting any value other than None automatically enables the signature. Selecting None disables the signature. If you chose None at this point and want to enable the signature later, you can do so by editing the Severity level again or enabling the signature through the Signature Groups panel. See "Enabling/Disabling/Editing Signatures Within a Group List" section on page 33 for more information.

- Information—Categorizes the attack as not relevant to security. These attacks are shown with a blue icon in the IDS Event Viewer.
- Low—Categorizes the attack as mildly severe. These attacks are shown with a yellow icon in the IDS Event Viewer.
- Medium—Categorizes the attack as moderately sever. These attacks are shown with a orange icon in the IDS Event Viewer.
- High—Categorizes the attack as highly severe. These attacks are shown with a red icon in the IDS Event Viewer.

Step 5 Select one or more of the **Action** check boxes to specify the actions that you want the sensor to take when detecting a particular attack:

Note Setting actions does not determine whether or not an alarm is logged or sent to an additional destination. See the "Configuring Event Logging" section on page 88 and/or "Adding Remote Hosts" section on page 24 for more information.

- Block—The sensor issues a command to a PIX Firewall or Cisco router. That device then denies the host or network from which the attack originated entry to the monitored network.
- IP Log—The sensor generates an IP session log with information about the attack. An IP session log contains binary data for all packets to and from the source address of the alarm.

Caution Generation of IP logs slows down the performance of the sensor. Use only when necessary.

Caution You do not have to set the action to IP Log to log the alarm. You only need the IP Log action if you want to log the binary packets to an IP log file.

- TCP Reset—The sensor resets the TPC session in which the attack signature was detected.

Note For the alarm to take no actions for that signature, deselect all the check boxes. Some actions are not available for each signature.

Step 6 Add any appropriate comments in the Comments field.

Note Add a name for the new UDP connection signature in the Comments field.

Step 7 Click **OK**.

Step 8 To enable the UDP connection signature that you just added, find the new signature in the list of UDP signatures, select the checkbox next to it, and then click **Enable**.

String Signatures

String-matching signatures are user-configurable signatures based on the content of a particular TCP session. You can enable/disable signatures, change the severity level or action associated with a signature, and add new string-matching signatures.

Note We recommend that you add new string-matching signatures through the Custom Signatures panel by using the STRING.* signature engines. See the "Working with Custom Signatures" section on page 38 for the procedure. When you add them as custom signatures, they appear in the list of Customer Signatures. Or refer to *Cisco Intrusion Detection System Signature Engines Version 3.1* found at the following website for more information on creating STRING.* signatures: http://www.cisco.com/univercd/cc/td/doc/product/iaabu/csids/csids8/index.htm

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1141
Fls:
3701
Doc:

This section includes these topics:

- Configuring String-Matching Signatures, page 58
- Adding a String-Matching Signature, page 60

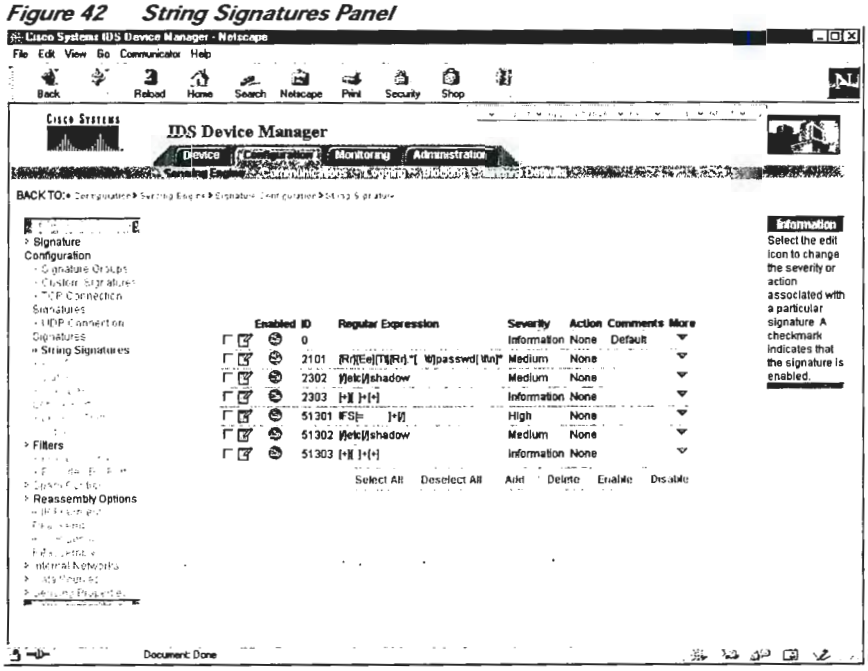
Configuring String-Matching Signatures

To configure string-matching signatures, follow these steps:

Step 1 In the IDS Device Manager main window, select **Configuration > Sensing Engine > String Signatures**.

Result: The String Signatures panel appears.

Figure 42 String Signatures Panel



Step 2 Select the signature(s) check box that you want to enable, and then click **Enable**.

Result: The circle is now solid indicating that the signature is enabled.

Note Enabling a signature sets the severity for that signature to its default severity level.

Step 3 Select the signature(s) check box that you want to disable, and then click **Disable**.

Result: The circle is now clear indicating that the signature is disabled.

Step 4 Select signature(s) check box that you want to delete, and then click **Delete**.

Result: The signature has disappeared from the list.

Note Disabling a signature sets the severity level for that signature to None.

4.150
CPL

Step 5 Click the edit icon to change the severity level or action for a string signature.

Result: The Editing panel appears.

Figure 43 Editing Panel

Step 6 To change the port number, enter a new value in the Port field.

Step 7 To change the direction of traffic to be monitored, use the list box in the Direction field:

- To specified port—Specifies that incoming packets should be searched for the defined string.
- From specified port—Specifies that outgoing packets should be searched for the defined string.
- Both directions—Specifies that both incoming and outgoing packets should be searched for the defined string.

Step 8 To change the number of occurrences of the string that causes the sensor to generate an alarm, enter a new value in the Occurrences field.

Step 9 To edit the string, change the value in the Regular expression field.

Step 10 Add any appropriate comments in the Comments field.

Step 11 From the Severity list box, select the severity level of the signature:

- None

Note Selecting any value other than None automatically enables the signature. Selecting None disables the signature. If you chose None at this point and want to enable the signature later, you can do so by editing the Severity level again or enabling the signature through the Signature Groups panel. See "Enabling/Disabling/Editing Signatures Within a Group List" section on page 33 for more information.

- Information—Categorizes the attack as not relevant to security. These attacks are shown with a blue icon in the IDS Event Viewer.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1142
Fls:
3701
Doc:

- Low—Categorizes the attack as mildly severe. These attacks are shown with a yellow icon in the IDS Event Viewer.
- Medium—Categorizes the attack as moderately sever. These attacks are shown with a orange icon in the IDS Event Viewer.
- High—Categorizes the attack as highly severe. These attacks are shown with a red icon in the IDS Event Viewer.

Step 12 Select one or more of the **Action** check boxes to specify the actions that you want the sensor to take when detecting a particular attack:

Note Setting actions does not determine whether or not an alarm is logged or sent to an additional destination. See the "Configuring Event Logging" section on page 88 and/or "Adding Remote Hosts" section on page 24 for more information.

- Block—The sensor issues a command to a PIX Firewall or Cisco router. That device then denies the host or network from which the attack originated entry to the monitored network.
- IP Log—The sensor generates an IP session log with information about the attack. An IP session log contains binary data for all packets to and from the source address of the alarm.

Caution Generation of IP logs slows down the performance of the sensor. Use only when necessary.

Caution You do not have to set the action to IP Log to log the alarm. You only need the IP Log action if you want to log the binary packets to an IP log file.

- TCP Reset—The sensor resets the TPC session in which the attack signature was detected.

Note For the alarm to take no actions for that signature, clear all the check boxes. Some actions are not available for each signature.

Note To reset the form, click **Reset**.

Step 13 Click **OK**.

Adding a String-Matching Signature

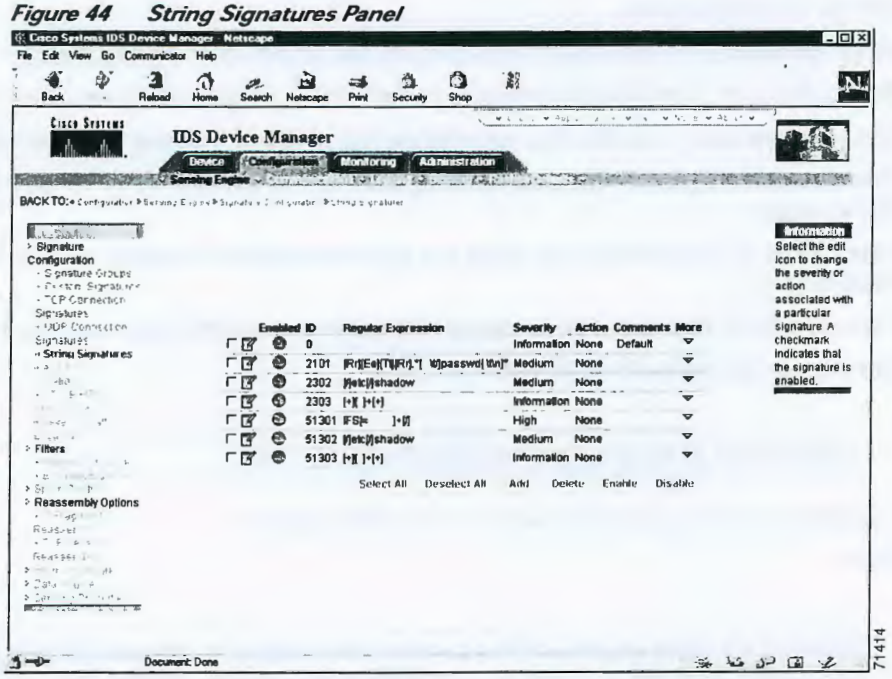
To add a string-matching signature, follow these steps:

Step 1 In the IDS Device Manager main window, select **Configuration > Sensing Engine > String Signatures**.

Result: The String Signatures panel appears.

E C
14.248
1
CPL - AC

Figure 44 String Signatures Panel



Step 2 Click **Add** to add a new string signature.

Result: The Adding panel appears.

Figure 45 Adding Panel

Step 3 Enter the ID number for the new signature.

Value: (1–65535)

RGS Nº 03/2005 - CN
CPMI - CORREIOS
1143
Fls:
3701
Doc:

Step 4 Enter the port in the Port field.

Step 5 To specify the direction of traffic to be monitored, use the list box in the Direction field:

- To specified port—Specifies that incoming packets should be searched for the defined string.
- From specified port—Specifies that outgoing packets should be searched for the defined string.
- Both directions—Specifies that both incoming and outgoing packets should be searched for the defined string.

Step 6 Enter the number of occurrences of the string that causes the sensor to generate an alarm in the Occurrences field.

Step 7 Enter the string to be used for the new string-matching signature in the Regular expression field.

Step 8 Add any appropriate comments in the Comments field.

Note Add the name of the new signature in the Comments field.

Step 9 From the Severity list box, select the severity level of the signature:

- None

Note Selecting any value other than None automatically enables the signature. Selecting None disables the signature. If you chose None at this point and want to enable the signature later, you can do so by editing the Severity level again or enabling the signature through the Signature Groups panel. See "Enabling/Disabling/Editing Signatures Within a Group List" section on page 33 for more information.

- Information—Categorizes the attack as not relevant to security. These attacks are shown with a blue icon in the IDS Event Viewer.
- Low—Categorizes the attack as mildly severe. These attacks are shown with a yellow icon in the IDS Event Viewer.
- Medium—Categorizes the attack as moderately sever: These attacks are shown with a orange icon in the IDS Event Viewer.
- High—Categorizes the attack as highly severe. These attacks are shown with a red icon in the IDS Event Viewer.

Step 10 Select one or more of the **Action** check boxes to specify the actions that you want the sensor to take when detecting a particular attack:

Note Setting actions does not determine whether or not an alarm is logged or sent to an additional destination. See the "Configuring Event Logging" section on page 88 and/or "Adding Remote Hosts" section on page 24 for more information.

- Block—The sensor issues a command to a PIX Firewall or Cisco router. That device then denies the host or network from which the attack originated entry to the monitored network.
- IP Log—The sensor generates an IP session log with information about the attack. An IP session log contains binary data for all packets to and from the source address of the alarm.

Caution Generation of IP logs slows down the performance of the sensor. Use only when necessary.

E C
4.146
I
AC

Caution You do not have to set the action to IP Log to log the alarm. You only need the IP Log action if you want to log the binary packets to an IP log file.

- TCP Reset—The sensor resets the TPC session in which the attack signature was detected.

Note For the alarm to take no actions for that signature, deselect all the check boxes. Some actions are not available for each signature.

Note To reset the form, click **Reset**.

Step 11 Click **OK**.

Step 12 To enable the new string-matching signature, find the new string signature in the String Signatures list, select the check box, and then click **Enable**.

ACL Policy Violation Signatures

ACL policy violation signatures are user-configurable signatures based on access control violations by network devices in the syslog stream.

You can configure two types of ACLs:

- User defined ACLs—Created and updated by users
- IDS defined ACLs—Created and updated by IDS Device Manager device management

There are no default ACL policy violation signatures when you configure a sensor for the first time. You must create ACL policy violation signatures, and you can modify them after you create them.

This section includes these topics:

- Configuring User-Defined ACLs, page 63
- Configuring IDS-Defined ACLs, page 70
- Enabling/Disabling/Deleting ACL Policy Violations Signatures, page 67
- Editing ACL Policy Violations Signatures, page 68

Configuring User-Defined ACLs

To configure user-defined ACLs, follow these steps:

Step 1 Log on to the router and enter enable mode by typing `en` and the enable password.

Step 2 Enter configuration mode by typing:

```
conf t
```

Step 3 Type the following commands:

`logging` *sensor_ip_address*

```
logging trap info
```

where *sensor_ip_address* is the IP address of the command and control interface of the sensor.

ROS Nº 03/2005 - CN
CPMI - CORREIOS
Fls:- 1144
3701
Doc:

Step 4 Exit configuration mode by pressing Ctrl-Z.

Step 5 To make the changes permanent on the router, type:

```
wr mem
```

Step 6 Set the user-defined ACLs on each router to send policy violation information by adding the text string "log" to the end of each line that defines a deny rule. For example:

```
access-list 199 deny tcp host 10.1.1.1 any log
```

This rule denies TCP traffic between host 10.1.1.1 and "any" other host. The string "log" at the end of the deny rule ensures that the policy violation is logged.

Note Rules that do not contain the text string "log" at the end of the line cause the router not to log the policy violation.

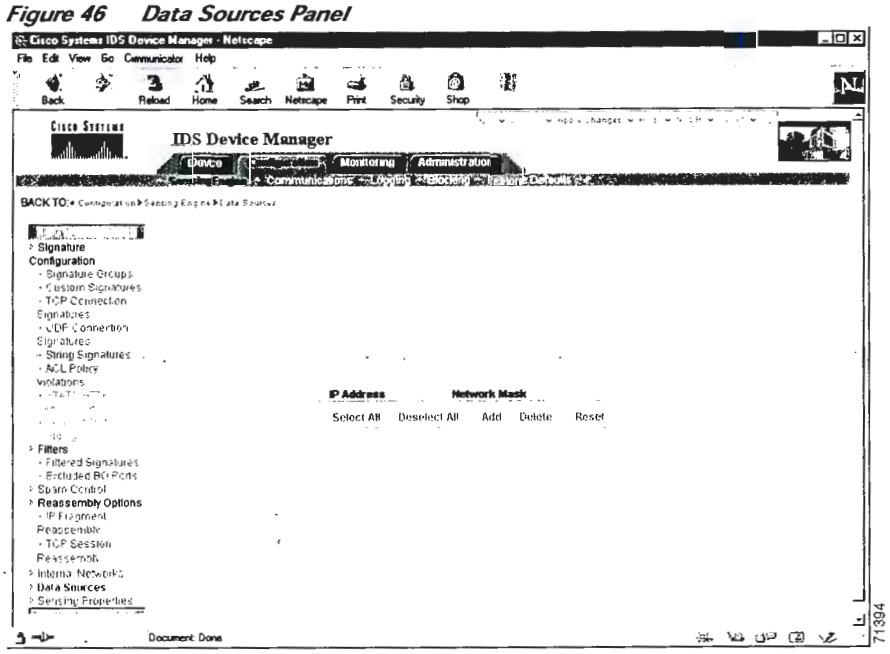
Step 7 To make the changes permanent on the router, type:

```
wr mem
```

Step 8 In the IDS Device Manager main window, select **Configuration > Sensing Engine > Data Sources**.

Result: The Data Sources panel appears.

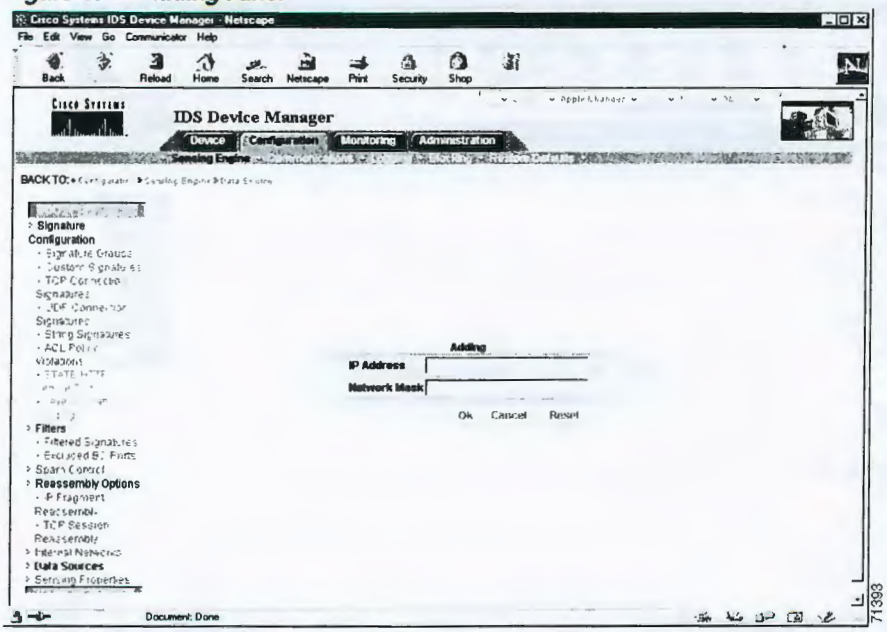
Figure 46 Data Sources Panel



Step 9 Click **Add** to add a data source.

Result: The Adding panel appears.

Figure 47 Adding Panel



Step 10 In the IP Address field, enter the IP address of the router that will publish syslog data to the sensor.

Step 11 In the Network Mask field, enter 255.255.255.255 if it is an IP address.

Note If you are monitoring syslogs from multiple routers on the same network, enter the network address and the netmask rather than the single IP address of each router.

Note To reset the form, click **Reset**.

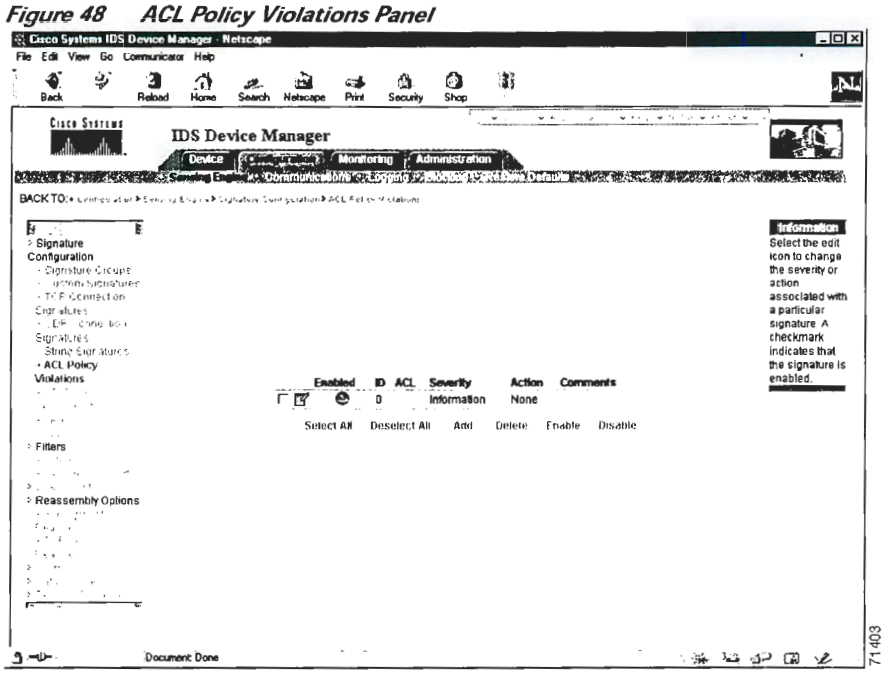
Step 12 Click **OK**.

Step 13 In the IDS Device Manager main window, select **Configuration > Sensing Engine > ACL Policy Violations**.

Step 14 Result: The ACL Policy Violations panel appears.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1145
Doc:

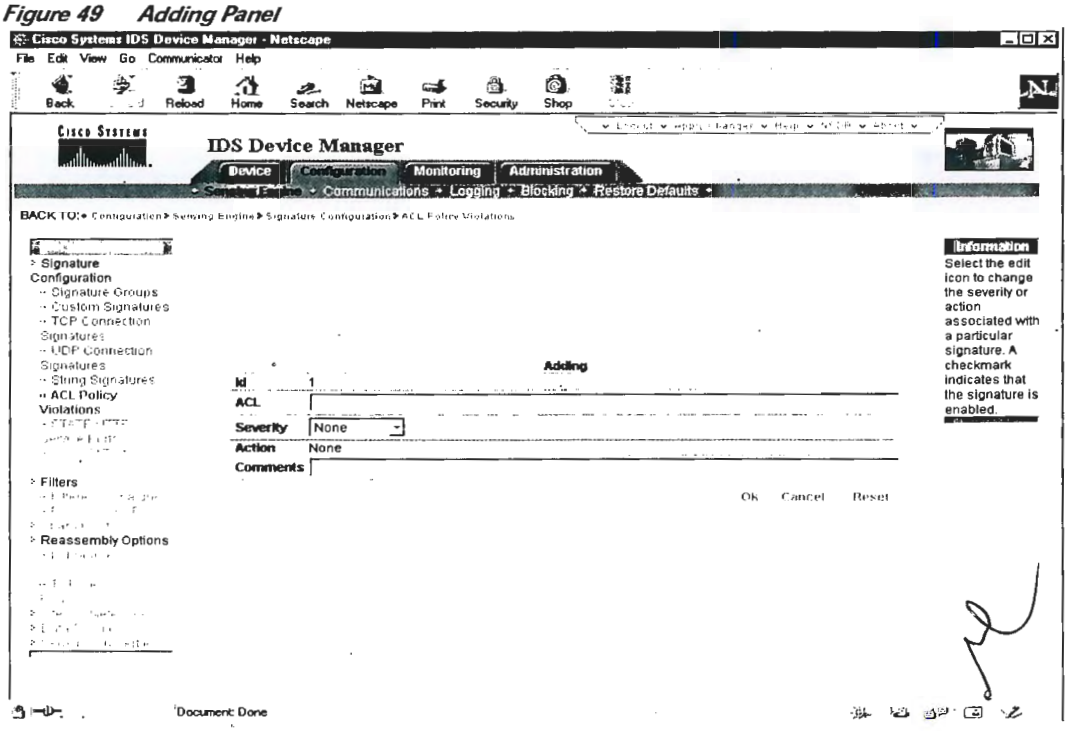
Figure 48 ACL Policy Violations Panel



Step 15 Click **Add** to add a new ACL policy violations signature.

Result: The Adding panel appears.

Figure 49 Adding Panel



Step 16 Enter the name or the number of the new ACL in the ACL field.

E C
4142
CPL - AC

Step 17 From the Severity list box, select the severity level of the signature:

- None

Note Selecting any value other than None automatically enables the signature. Selecting None disables the signature. If you chose None at this point and want to enable the signature later, you can do so by editing the Severity level again or enabling the signature through the Signature Groups panel. See "Enabling/Disabling/Editing Signatures Within a Group List" section on page 33 for more information.

- Information—Categorizes the attack as not relevant to security. These attacks are shown with a blue icon in the IDS Event Viewer.
- Low—Categorizes the attack as mildly severe. These attacks are shown with a yellow icon in the IDS Event Viewer.
- Medium—Categorizes the attack as moderately sever. These attacks are shown with a orange icon in the IDS Event Viewer.
- High—Categorizes the attack as highly severe. These attacks are shown with a red icon in the IDS Event Viewer.

Step 18 Add any appropriate comments in the Comments field.

Note To reset the form, click **Reset**.

Step 19 Click **OK**.

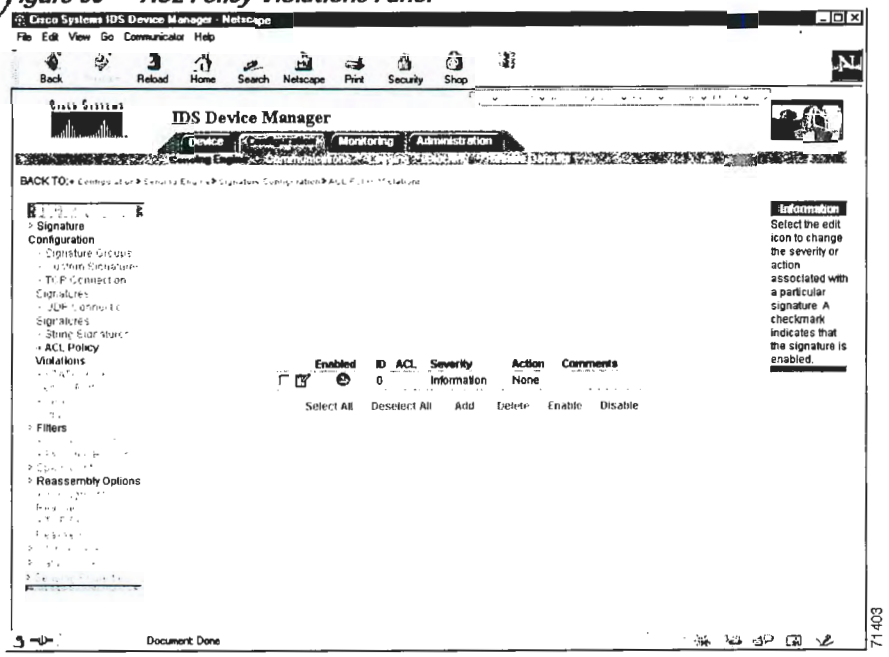
Enabling/Disabling/Deleting ACL Policy Violations Signatures

Step 1 In the IDS Device Manager main window, select **Configuration > Sensing Engine > ACL Policy Violations**.

Step 2 Result: The ACL Policy Violations panel appears.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1146
Doc: 3701

Figure 50 ACL Policy Violations Panel



Step 3 To enable the new ACL policy violations signature, select the signature(s) check box, and then click **Enable**.

Result: The circle is now solid indicating that the signature is enabled.

Note Enabling a signature sets the severity for that signature to its default severity level.

Step 4 To disable the new ACL policy violations signature, select the signature(s) check box, and then click **Disable**.

Result: The circle is now clear indicating that the signature is disabled.

Note Disabling a signature sets the severity level for that signature to None.

Step 5 To delete the new ACL policy violations signature, select the signature(s) check box, and then click **Delete**.

Result: The signature has disappeared from the list.

Editing ACL Policy Violations Signatures

Step 1 In the IDS Device Manager main window, select **Configuration > Sensing Engine > ACL Policy Violations**.

Step 2 Result: The ACL Policy Violations panel appears.

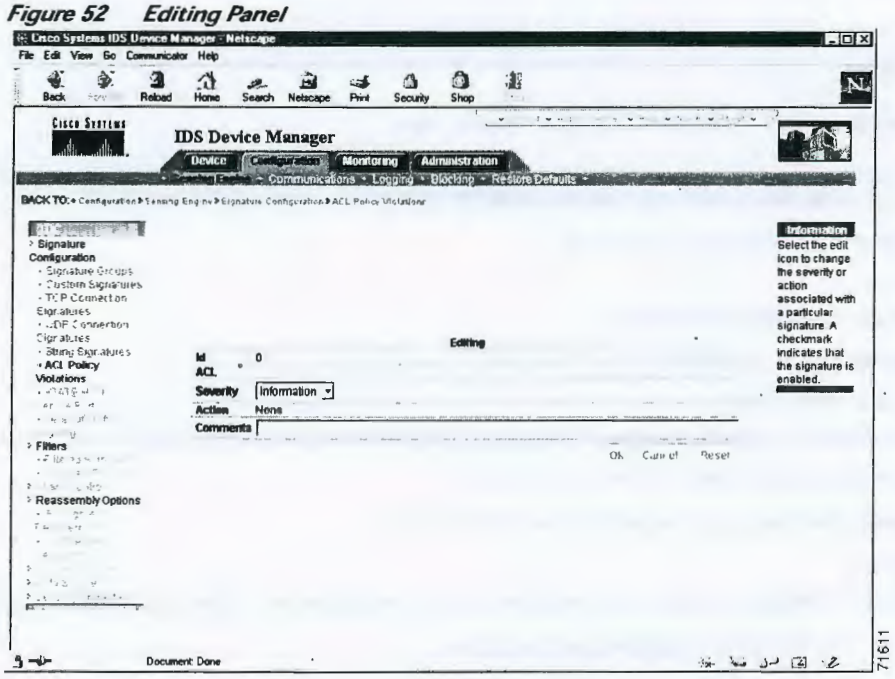
1140
CPL - AC

Figure 51 ACL Policy Violations Panel

Step 3 Click the edit icon to edit an ACL policy violations signature.

Result: The Editing panel appears.

Figure 52 Editing Panel



RQS Nº 03/2005 - CN
CPMI - CORREIOS
1147
Fls:
3701
Doc:

Step 4 From the Severity list box, select the severity level of the signature:

- None

Note Selecting any value other than None automatically enables the signature. Selecting None disables the signature. If you chose None at this point and want to enable the signature later, you can do so by editing the Severity level again or enabling the signature through the Signature Groups panel. See "Enabling/Disabling/Editing Signatures Within a Group List" section on page 33 for more information.

- Information—Categorizes the attack as not relevant to security. These attacks are shown with a blue icon in the IDS Event Viewer.
- Low—Categorizes the attack as mildly severe. These attacks are shown with a yellow icon in the IDS Event Viewer.
- Medium—Categorizes the attack as moderately sever. These attacks are shown with a orange icon in the IDS Event Viewer.
- High—Categorizes the attack as highly severe. These attacks are shown with a red icon in the IDS Event Viewer.

Step 5 Add any appropriate comments in the Comments field.

Note To reset the form, click **Reset**.

Step 6 Click **OK**.

Configuring IDS-Defined ACLs

To configure IDS-Defined ACLs, follow these steps:

Step 1 Log on to the router and enter enable mode by typing `en` and the enable password.

Step 2 Enter configuration mode by typing:

```
conf t
```

Step 3 Type the following commands:

`logging` *sensor_ip_address*

```
logging trap info
```

where *sensor_ip_address* is the IP address of the command and control interface of the sensor.

Step 4 Exit configuration mode by pressing **Ctrl-Z**.

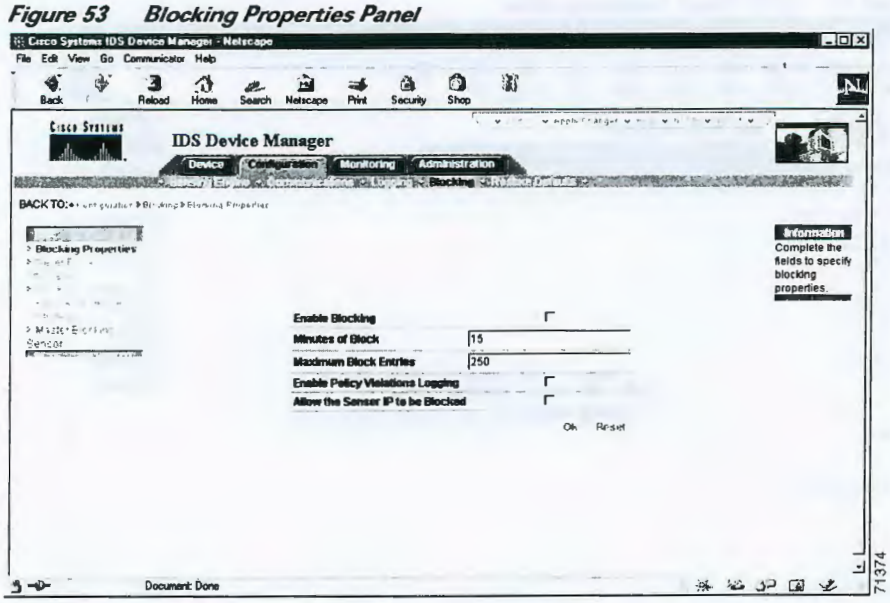
Step 5 To make the changes permanent on the router, type:

```
wr mem
```

Step 6 In the IDS Device Manager main window, select **Configuration** > **Blocking** > **Blocking Properties**.

Step 7 Result: The Blocking Properties panel appears.

Figure 53 Blocking Properties Panel



Step 8 Select the **Enable Policy Violations Logging** check box to enable the logging of ACL policy violations on the blocking device

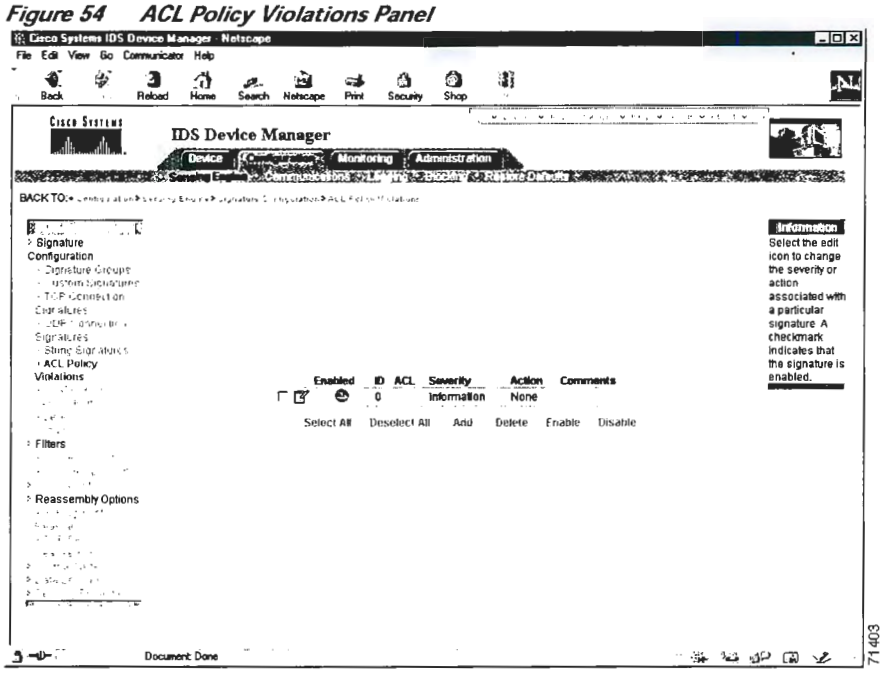
Step 9 Click **OK**.

Step 10 In the IDS Device Manager main window, select **Configuration > Sensing Engine > ACL Policy Violations**.

Step 11 Result: The ACL Policy Violations panel appears.

ROS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1148
Doc: 3701

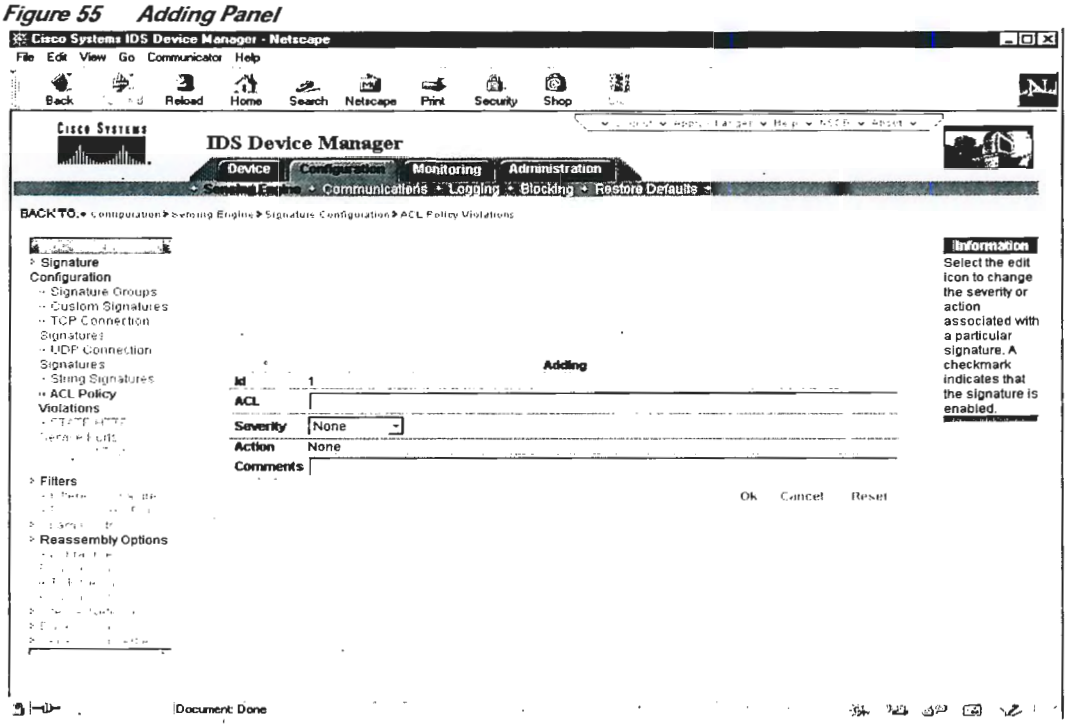
Figure 54 ACL Policy Violations Panel



Step 12 Click **Add** to add a new ACL policy violations signature.

Result: The Adding panel appears.

Figure 55 Adding Panel



Step 13 Enter the name of the new ACL in the ACL field.

Value: IDS_*interface_direction*_0

Note *Interface* is the name of the interface that the sensor is managing. *Direction* is IN/OUT.

Step 14 From the Severity list box, select the severity level of the signature:

- None

Note Selecting any value other than None automatically enables the signature. If you chose None at this point and want to enable the signature later, you can do so by editing the Severity level again or enabling the signature through the Signature Groups panel. See "Enabling/Disabling/Editing Signatures Within a Group List" section on page 33 for more information.

- Information—Categorizes the attack as not relevant to security. These attacks are shown with a blue icon in the IDS Event Viewer.
- Low—Categorizes the attack as mildly severe. These attacks are shown with a yellow icon in the IDS Event Viewer.
- Medium—Categorizes the attack as moderately sever. These attacks are shown with a orange icon in the IDS Event Viewer.
- High—Categorizes the attack as highly severe. These attacks are shown with a red icon in the IDS Event Viewer.

Step 15 Add any appropriate comments in the Comments field.

Step 16 Click **OK**.

Step 17 Repeat Steps 9–13 for the second ACL.

Value: IDS_*interface_direction*_1

Note The sensor device management oscillates between the 0 and 1 ACLs. You need both of them and you must enter them as separate signatures.

Choosing Service Ports for STATE.HTTP Signatures

If you are running a web server on nonstandard HTTP ports, use the Service Ports panel to add those ports.

You need to configure the signatures for the STATE.HTTP engine to specific service ports. For more information on the STATE.HTTP signature engine, refer to the *Cisco Intrusion Detection System Signature Engines Version 3.1* found at the following website:

http://www.cisco.com/univercd/cc/td/doc/product/iaabu/csids/csids8/index.htm

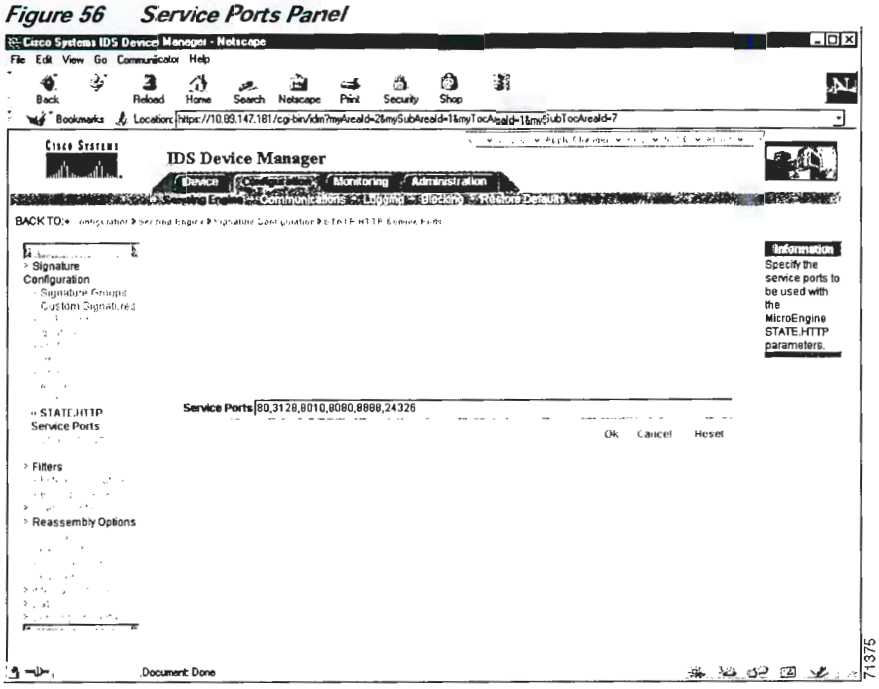
RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1149
3701
Doc:

To choose service ports, follow these steps:

Step 1 In the IDS Device Manager main window, select **Configuration > Sensing Engine > STATE.HTTP Service Ports**.

Result: The STATE.HTTP Service Ports panel appears.

Figure 56 Service Ports Panel



Step 2 In the Service Ports field, enter the service ports (separated by commas) that you want to use with the STATE-HTTP engine.

Default: 80,3128,8010,8080,8888,24326

Note We recommend that you edit the default list to turn off ports that you are sure you are not using. For example, if you are only using port 80, delete the other entries.

Note To reset the form, click **Reset**.

Step 3 Click **OK**.

Configuring the Level of Traffic Logging

Level of Traffic Logging is used in conjunction with the TCP and UDP connection signatures. It configures what type of packets cause the TCP and UDP connection signatures to fire alarms.

To configure the level of traffic logging, follow these steps:

Step 1 In the IDS Device Manager main window, select **Configuration > Sensing Engine > Level of Traffic Logging**.

Result: The Level of Traffic Logging panel appears.

Figure 57 Level of Traffic Logging Panel

Step 2 In the Level of Traffic Logging field, specify the level of traffic you want the sensor to log when TCP and UDP connection signatures are enabled:

- None—Disables logging.

  No TCP or UDP connection signatures will fire even it enabled.

- TCP connection requests and UDP traffic (default).

  The TCP connection signatures that are enabled will fire for SYN packets to the specific port. The UDP connection signatures that are enabled will fire for any UDP packet to those ports.

- TCP connection requests, SYN-ACK, FIN, RST, and UDP traffic.

- TCP SYN-ACK packets from the specified port and UDP traffic.

  Use this option to configure TCP reset action for TCP connection signatures.

Note To reset the form, click **Reset**.

Step 3 Click **OK**.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1150
3701
Doc:

Creating Filters

You can define filters for a sensor to enable and disable alarms that have specific hosts and networks as their source or destination. Defining filters allows you to tune the sensor by reducing the number of false positives. You can also define filters to disable alarms based on a particular traffic flow that traverses the network segment that is being monitored. In this case you are defining traffic flow based on the source and destination that bounds the traffic flow.

You can exclude signatures to disable alarms based on signature ID, IP address, and direction that includes the following:

- Exclude a signature.
- Exclude a source or destination IP address or network.
- Exclude a specific source and destination IP address or network.
- Exclude a specific signature by source and/or destination IP address.
- Exclude a signature based on source and/or destination direction (for example, IN or OUT).

Note CSPM and the IDS Director may have created filters using older configuration formats. The IDS Device Manager reads in and writes out these filters, but you cannot view, edit, or delete them through the IDS Device Manager.

You can also define a set of ports that will be excluded from triggering a Back Orifice 2K TCP alarm. You can configure these TCP ports to exclude alarms from the TCP port BO2K signatures (signatures 3990, 3991, 3992). The UDP ports are unaffected (signatures 4054 and 5044). For more information on these signatures, click **NSDB** on the ToolBar and then click the signatures IDs **3990**, **3991**, and **3992**.

This section includes these topics:

- Configuring Filters, page 76
- Configuring Excluded BO Ports, page 78

Configuring Filters

To configure filters for enabled signatures, follow these steps:

Step 1 In the IDS Device Manager main window, select **Configuration > Sensing Engine > Filters > Filtered Signatures**.

Result: The Filtered Signatures panel appears.

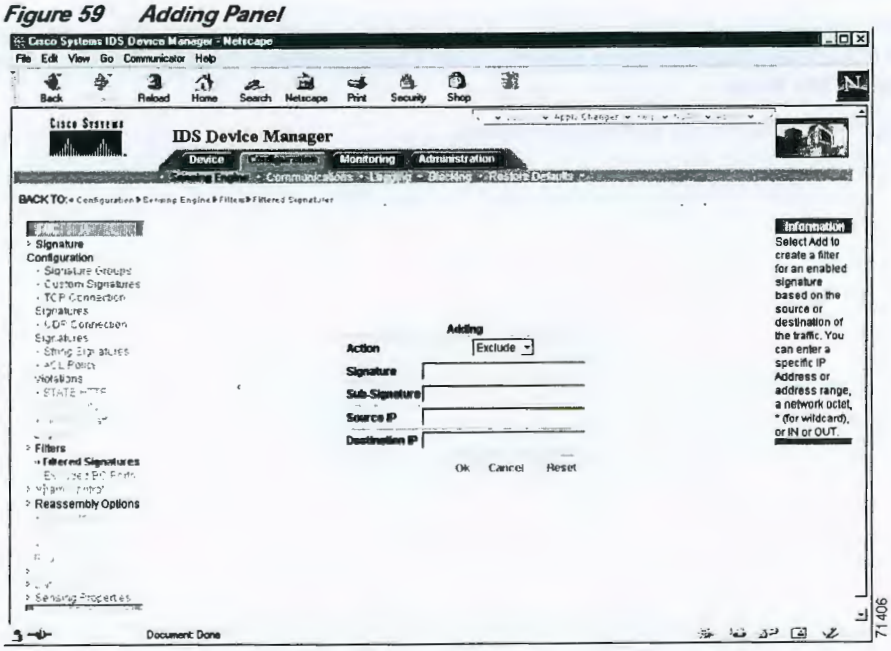
4-132

Figure 58 Filtered Signatures Panel

Step 2 Click **Add** to configure a filter for an enabled signature based on the source or destination of the traffic.

Result: The Adding panel appears.

Figure 59 Adding Panel



Step 3 Select one of the following from the Action list box:

- Include
- Exclude

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1151
Fls: 3701
Doc:

Note Include/exclude specifies whether the identified signature for the source/destination pair should be included or excluded. Includes are used to override excludes. In typical scenarios you exclude all addresses for a given alarm, and then add an include only for those addresses you want the alarm to fire on.

Step 4 In the Signature field, enter the signature that should be included or excluded.

Step 5 In the Sub-Signature field, enter the subsignature (if applicable) of the signature that should be included or excluded.

Note If you enter multiple signatures, the value must be an '*'.

Step 6 In the Source IP field, enter the source IP address of traffic that triggers the signature or subsignature.

Step 7 In the Destination IP field, enter the destination IP address of traffic that triggers the signature or subsignature.

Note To reset the form, click **Reset**.

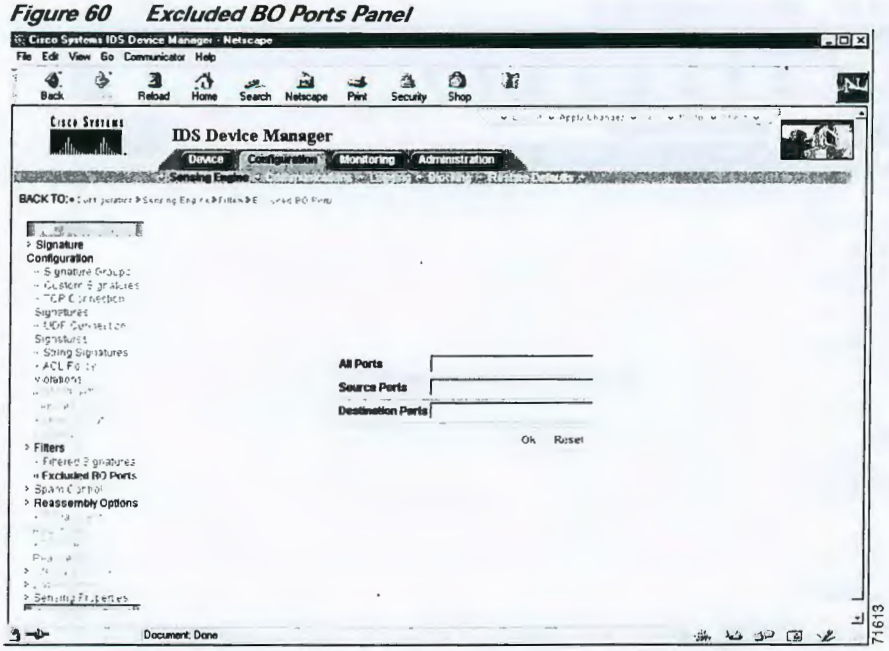
Step 8 Click **OK**.

Configuring Excluded BO Ports

Step 1 In the IDS Device Manager main window, select **Configuration > Sensing Engine > Filters > Excluded BO Ports**.

Result: The Excluded BO Ports panel appears

Figure 60 Excluded BO Ports Panel



Step 2 In the All Ports field, enter the ports that you do not want to trigger BO signatures.

Note Packets moving in either direction on these ports will not trigger BO signatures. The values may be a single port, a range of ports (port-port), or a list of comma-delimited ports and port ranges. Do not use spaces.

Step 3 In the Source Ports field, enter the source ports that you do not want to trigger BO signatures.

Step 4 In the Destination Ports field, enter the destination ports that you do not want to trigger BO signatures.

Step 5 Click **OK**.

Configuring Spam Control

You can limit the number of recipients in email messages.

To configure spam control, follow these steps:

Step 1 In the IDS Device Manager main window, select **Configuration > Sensing Engine > Spam Control**.

Result: The Spam Control panel appears.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1152
Doc: 370

Figure 61 Spam Control Panel

Step 2 In the Max number of Recipients in a Mail Message field, enter a number between 2-65000.

Default: 250

Note To reset the form, click **Reset**.

Step 3 Click OK.

Reassembly Options

You can configure the sensor to reassemble a datagram that has been fragmented over multiple packets. You can specify boundaries that the senor uses to determine how many datagrams, how many fragments per datagram, and how long to wait for more fragments of a datagram. The goal is to ensure that the sensor does not allocate all of its resources to datagrams that cannot be completely reassembled, either because the sensor missed some frame transmissions or because an attack has been launched that is based on generating random fragment datagrams.

You can configure the sensor to only monitor TCP sessions that have been established by a complete three-way handshake. You can also configure how long to wait for the handshake to complete, and how long to keep monitoring a connection where no more packets have been seen. The goal is to prevent the sensor from creating alarms where a valid TCP session has not been established. There are known attacks against IDS systems that try to get the IDS to generate alarms by simply replaying pieces of an attack. The TCP session reassembly feature helps to mitigate these types of attacks against the IDS.

This section includes these topics:

- Configuring IP Fragment Reassembly, page 81
- Configuring TCP Session Reassembly, page 82

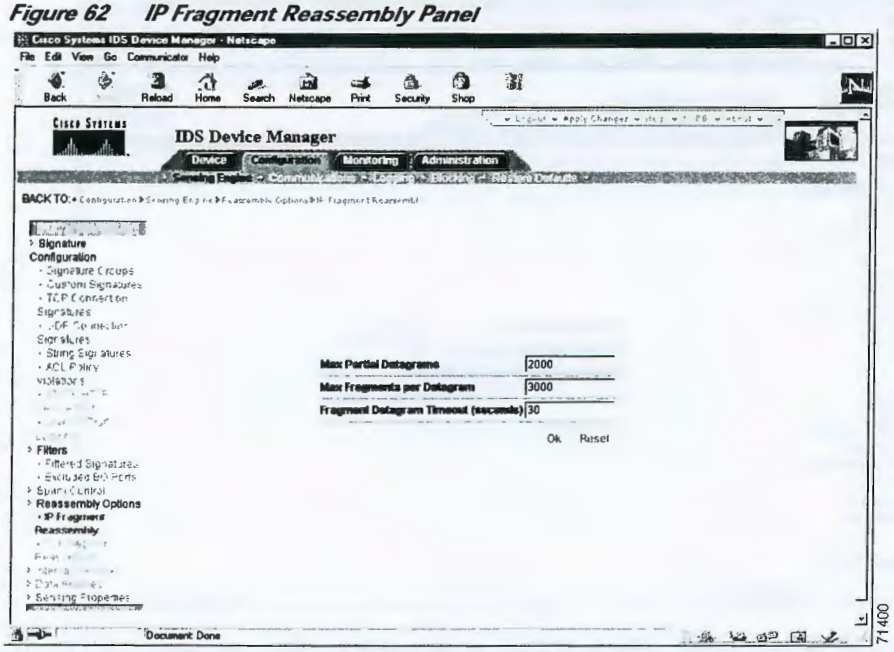
Configuring IP Fragment Reassembly

To configure IP fragment reassembly, follow these steps:

Step 1 In the IDS Device Manager main window, select **Configuration > Sensing Engine > Reassembly Options > IP Fragment Reassembly**.

Result: The IP Fragment Reassembly panel appears.

Figure 62 IP Fragment Reassembly Panel



Step 2 In the Max Partial Datagrams field, enter a numerical value between 1 and 65000 to specify the maximum number of partial datagrams the sensor can attempt to reconstruct at one time.

Default: 2000

Step 3 In the Max Fragments per Datagram field, enter a numerical value between 1 and 3000 to specify the maximum number of fragments that can be accepted into a single datagram.

Default: 3000

Step 4 In the Fragment Datagram Timeout field, enter a numerical value between 1 and 300 to specify the maximum number of seconds that can elapse before the sensor stops keeping track of a particular exchange for which it is trying to reassemble a datagram.

Default: 30

Note To reset the form, click **Reset**.

Step 5 Click **OK**.

RQS Nº 03/2005 - CN - CPMI - CORREIOS
Fls: 1153
Doc: 3701

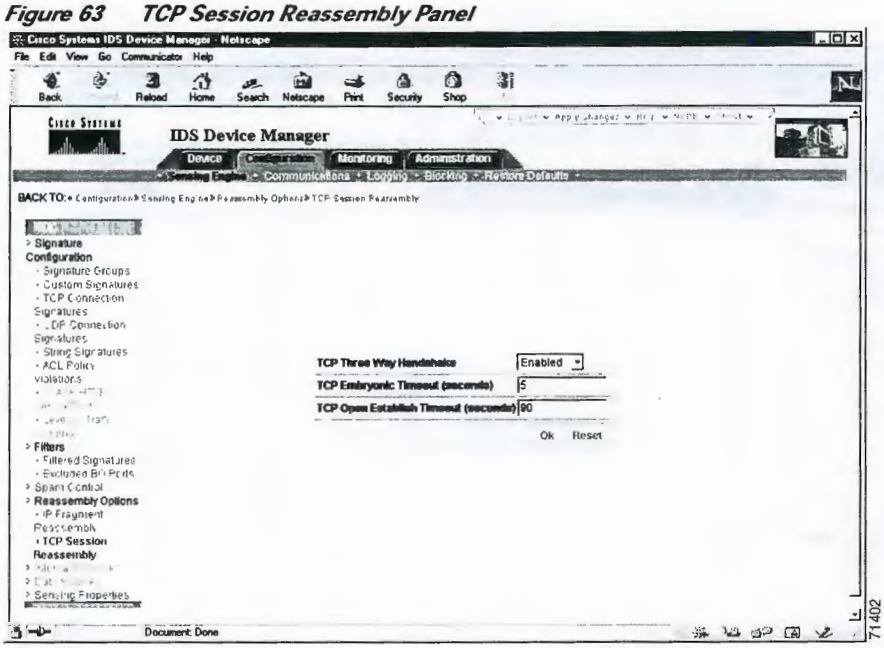
Configuring TCP Session Reassembly

To configure TCP session reassembly, follow these steps:

Step 1 Select **Configuration > Sensing Engine > Reassembly Options > TCP Session Reassembly**.

Result: The TCP Session Reassembly panel appears.

Figure 63 TCP Session Reassembly Panel



Step 2 To specify that the sensor track only sessions for which the three-way handshake is completed, select **Enabled** in the TCP Three Way Handshake list box.

Step 3 In the TCP Embryonic Timeout field, enter a numerical value between 1 and 180 to specify the number of seconds that can elapse before the sensor frees the resources allocated for an initiated, but not fully established, TCP session.

Default: 5

Step 4 In the TCP Open Establish Timeout field, enter a numerical value between 1 and 3600 to specify the number of seconds that can elapse before the sensor frees the resources allocated to a fully established TCP connection when no more packets are being seen for that connection.

Default: 90

Note To reset the form, click **Reset**.

Step 5 Click **OK**.

Configuring Internal Networks

You can identify internal networks for each sensor you manage with the IDS Device Manager. Internal network are networks you consider trusted. Internal networks are handled differently from external networks with regard to alarms and reports.

Internal networks may be represented by a simple IP address (10.1.1.1), a range of IP addresses (10.1.1.1–10.1.1.20), the IP address/bitmask (10.1.1.1/24), or the IP netmask (10.1.1.0 255.255.255.0).

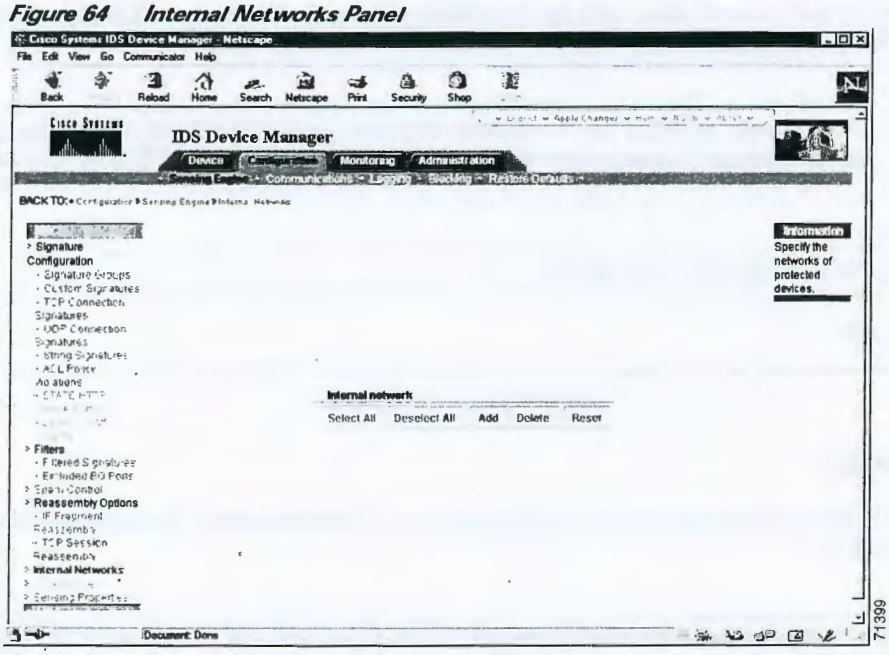
Note Addresses that are configured as internal networks are marked with the keyword IN when the alarm is generated. All other addresses are marked with the keyword OUT. You can use the IN and OUT keywords when creating filters. See the "Creating Filters" section on page 76 for more information.

To identify an internal network, follow these steps:

Step 1 In the IDS Device Manager main window, select **Configuration > Sensing Engine > Internal Networks**.

Result: The Internal Networks panel appears.

Figure 64 Internal Networks Panel

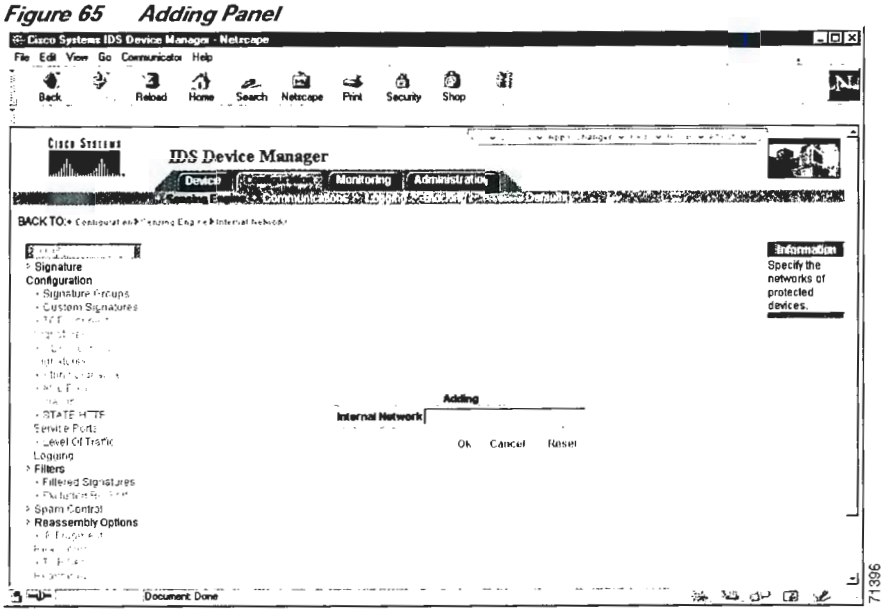


Step 2 Click **Add** to set up the IP addresses for protected devices.

Result: The Adding panel appears.

RDS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1154
3701
Doc:

Figure 65 Adding Panel



Step 3 In the Internal Network field, enter the IP address of the protected device or the beginning of the range of protected devices.

Note For example, to define the 10. network as internal, add 10.0.0.0 as the IP address and 255.0.0.0 as the netmask. To add a single host as internal, add for example, 172.21.10.22 as the IP address.

Note To reset the form, click **Reset**.

Step 4 Click **OK**.

Configuring Data Sources

A Cisco IOS router can publish syslog data to a sensor. You must specify the interface that the Cisco IOS router uses.

Note You must configure data sources when designating ACL policy violation signatures. See the "ACL Policy Violation Signatures" section on page 63 for more information.

Step 1 In the IDS Device Manager main window, select **Configuration > Sensing Engine > Data Sources**.

Result: The Data Sources panel appears.

G-124

Figure 66 Data Sources Panel

Step 2 Click **Add** to add a data source.

Result: The Adding panel appears.

Figure 67 Adding Panel

Step 3 In the IP Address field, enter the IP address of the interface of the router that will publish syslog data to the sensor, or the IP address of a network if multiple routers from the same network will be sending syslog data to the sensor.

ROS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1155
3701
Doc:

Step 4 In the Network Mask field, enter 255.255.255.255 if only a single router interface will publish syslog data to the sensor, or enter the netmask if a network was entered in Step 3.

Note To reset the form, click **Reset**.

Step 5 Click **OK**.

Configuring the Sensing Properties

You can use the Sensing Properties panel to specify the following:

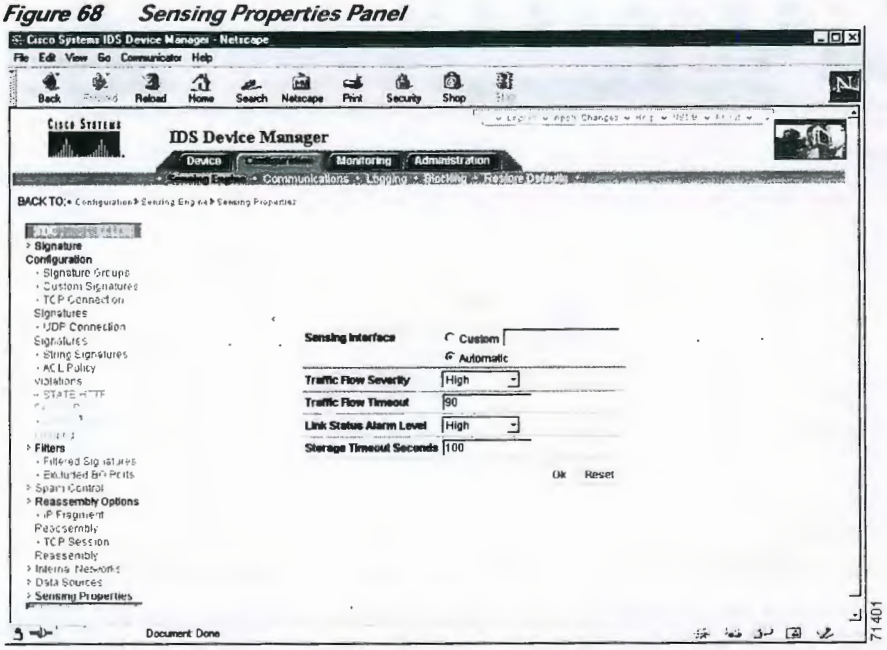
- Which interface to use for sensing.
- The severity of the alarm to generate when the sensing interface stops seeing packets for a specified amount of time.
- The severity of the alarm to generate when the sensing interface is physically disconnected from a switch or hub.
- How long the sensor will store information after no more packets are seen from a certain host.

To configure the sensing properties, follow these steps:

Step 1 In the IDS Device Manager main window, select **Configuration > Sensing Engine > Sensing Properties**.

Result: The Sensing Properties panel appears.

Figure 68 Sensing Properties Panel



Step 2 In the Sensing Interface field, select **Custom** or **Automatic** from the list box.

Note We recommend selecting Automatic, because it allows the sensor to determine the monitoring interface.

Note Select **Custom** if you need to do a manual override of the sensing interface device. You need to know the specific device name for your sensor.

Step 3 In the Traffic Flow Severity field, select the alarm severity level of the traffic flow alerts.

Default: 5

Note The sensor generates the 994 Have Traffic alarm with this severity when the sensing interface sees traffic. It generates the 995 No Traffic alarm with this severity when the sensing interface has not seen any traffic on the sensing interface for Traffic Flow Timeout seconds.

Step 4 In the Traffic Flow Timeout field, enter a numerical value between 0 and 65000 to specify the number of idle seconds before triggering a No Traffic Alert.

Default: 90

Step 5 In the Link Status Alarm Level field, select the alarm severity level of the link status alert.

Default: 5

Note The sensor generates the 995 No Traffic alarm with this severity if the sensing interface is physically disconnected from a switch or hub. The 994 Have Traffic alarm fires when it is reconnected and seeing packets. Currently, the IDS 4210 only has this ability.

Step 6 In the Storage Timeout Seconds field, enter a numerical value between 10 - 600 to specify the number of seconds to wait before deleting stored history, after the host goes silent.

Default: 300

Note To reset the form, click **Reset**.

Step 7 Click **OK**.

Configuring Logging

This section includes the following procedures:

- Configuring Event Logging, page 88
- Exporting Event Logs, page 89
- Configuring Automatic IP Logging, page 91
- Configuring IP Logging, page 92

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1156
3701
Doc:

Configuring Event Logging

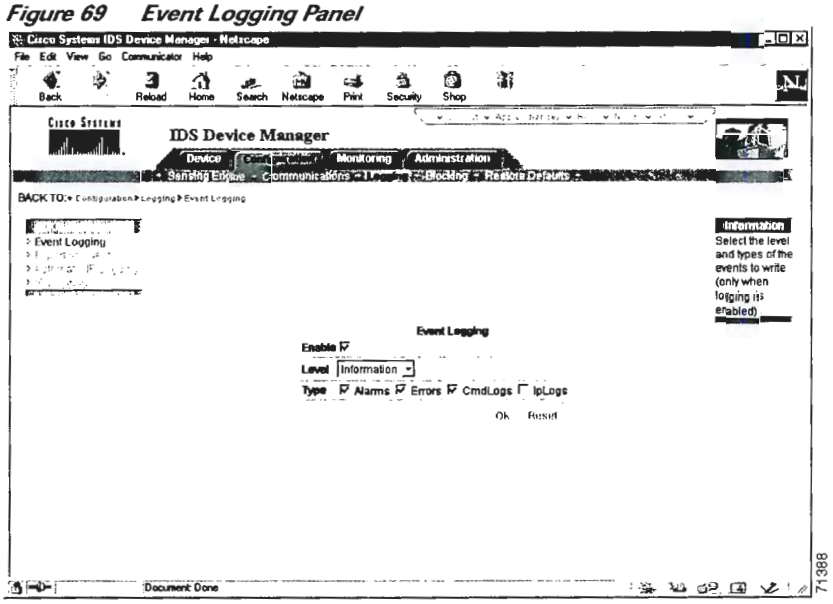
A sensor can generate audit event logs locally on the sensor based on network data streams, or syslog data streams, or both, depending on what the sensor has been configured to watch.

To configure how events will be logged, follow these steps:

Step 1 In the IDS Device Manager main window, select **Configuration > Logging > Event Logging**.

Result: The Event Logging panel appears.

Figure 69 Event Logging Panel



Step 2 Select the **Enable** check box.

Step 3 From the Level list box, select the severity level of the signature:

- Information—Categorizes the attack as not relevant to security. These attacks are shown with a blue icon in the IDS Event Viewer.
- Low—Categorizes the attack as mildly severe. These attacks are shown with a yellow icon in the IDS Event Viewer.
- Medium—Categorizes the attack as moderately sever. These attacks are shown with a orange icon in the IDS Event Viewer.
- High—Categorizes the attack as highly severe. These attacks are shown with a red icon in the IDS Event Viewer.

Step 4 Select one or more of the **Type** check boxes to specify types of events you want to log:

- Alarms
- Errors
- CmdLogs
- IPLogs

E
4.120
L

Note If you select alarm type, all alarms for enabled signatures with severities greater than or equal to the selected level are logged to the /usr/nr/var/log.*timestamp* file. You do not have to select a specific action for the signature.

Note You can only set the Level and Type options after you have enabled event logging. Alarms, Errors, and ComdLogs are written to the event log. IPLogs are stored separately. Select **Monitoring > Logs** to view the log files.

Caution If you select IPLogs, you must also set the severity level to Information. When an alarm occurs for signatures with an action of IPLog, all packets to and from the source address of the alarm are logged in a binary format in the /usr/ne/nr/iplog/iplog.*address.timestamp* files.

Note To reset the form, click **Reset**.

Step 5 Click **OK**.

Exporting Event Logs

You can specify an FTP server that event logs are sent to at regular intervals.

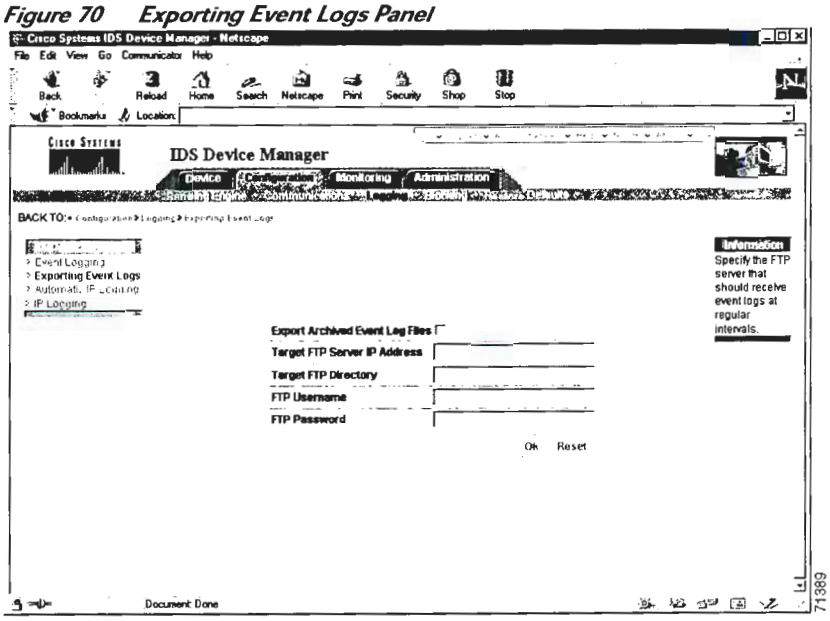
To export event logs, follow these steps:

Step 1 In the IDS Device Manager main window, select **Configuration > Logging > Exporting Event Logs**.

Result: The Exporting Event Logs panel appears.

RQS Nº 03/2005 - CN -
CPMI - CORREIOS
Fls: 115
3701
Doc:

Figure 70 Exporting Event Logs Panel



Step 2 Select the **Export Archived Event Log Files** check box.

Export Archived Event Log Files determines if the logs are automatically exported.

Note If the check box is selected, the sensor checks to see if local event logging has been enabled. If the check box is clear, a warning message is displayed.

Step 3 In the Target FTP Server IP Address field, enter the IP address of the FTP server you want to connect to and to send the logs to.

The following FTP servers support the FTP log export functions:

- Sambar FTP Server Version 5.0 (win32)
- Web-mail Microsoft FTP Service Version 5.0 (win32)
- Serv-U FTP-Server v2.5h for WinSock (win32)
- Solaris 2.8
- HP-UX (HP-UX qdir-5 B.10.20 A 9000/715)
- Windows 2000 (Microsoft ftp server version 5.0)
- Windows NT 4.0 (Microsoft ftp server version 3.0)

Step 4 In the Target FTP Directory field, enter the target directory on the remote FTP server (1 to 128 characters).

Step 5 In the FTP Username field, enter the FTP server login name (1 to 16 characters).

Step 6 In the FTP Password field, enter the FTP server password associated with the login name (1 to 8 characters).

Note To reset the form, click **Reset**.

Step 7 Click **OK**.

Step 8 Verify the event logs are being exported by viewing the messages.sapd file by selecting **Monitoring>Logs>Messages>sapd**.

Note Logs are FTPed every time the current event log is closed and archived. By default, this occurs once a day or when the logs fill up the 104876 bytes allocated to them, whichever comes first.

Configuring Automatic IP Logging

You can configure a sensor to generate an IP session log when the sensor detects an attack. When IP logging is configured as a response action for a signature and the signature is triggered, all packets to and from the source address of the alarm are logged for a specified period of time. You can set the number of minutes events are logged.

Note IP logging requires that event logging be enabled with Information as the severity level and at least IPLogs for the type.

To set the amount of minutes of automatic IP logging, follow these steps:

Step 1 In the IDS Device Manager main window, select **Configuration > Logging > Automatic IP Logging**.

Result: The Automatic IP Logging panel appears.

Figure 71 Automatic IP Logging Panel

Step 2 In the Minutes of IP Logging field, enter the number of minutes you want IP logging to be done (1 to 60).

Default: 15

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls:
Doc: 3701

Note To reset the form, click **Reset**.

Step 3 Click **OK**.

Step 4 Download the logs by selecting **Monitoring > Logs > IP Logs > Archived**.

Note The IP logs are in a binary TCP dump format. To view the contents of the logs, download them to your desktop, and run a tool like Ethereal to view the logged packets. You can download Ethereal from the following website:
www.ethereal.com

Configuring IP Logging

You can configure the sensor to capture all traffic related to the specified hosts. The IP logging option logs all traffic or a list of IP addresses.

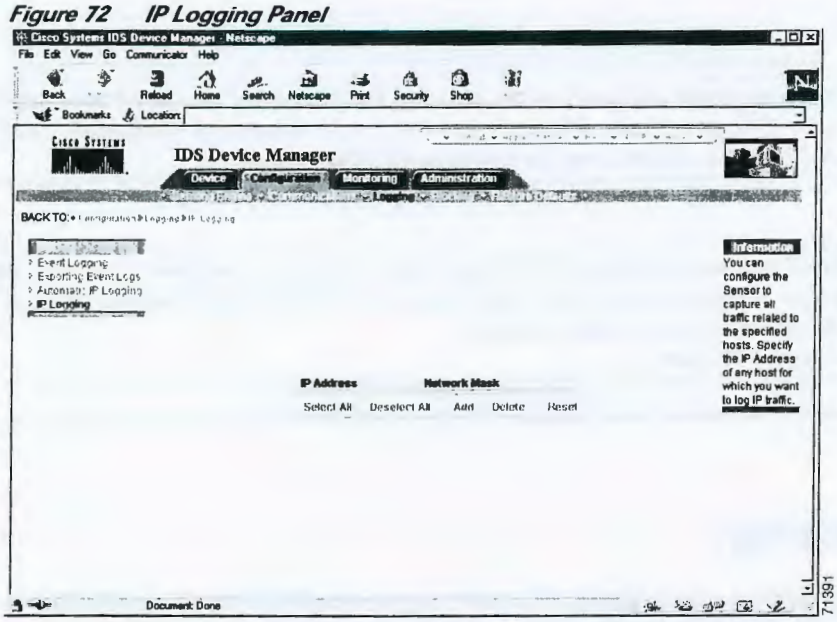
Note IP logging requires that event logging be enabled with Information as the severity level and at least IPLogs for the type.

To generate log files for specific IP addresses, follow these steps:

Step 1 In the IDS Device Manager main window, select **Configuration > Logging > IP Logging**.

Result: The IP Logging panel appears.

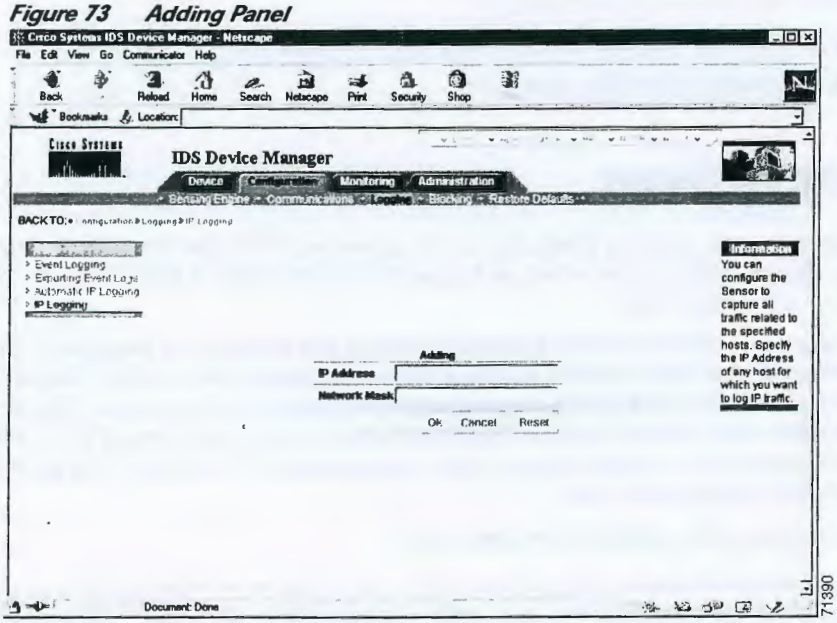
Figure 72 IP Logging Panel



Step 2 Click **Add** to enter IP addresses.

Result: The Adding panel appears.

Figure 73 Adding Panel



Step 3 In the IP Address field, enter the source IP address to log.

Step 4 In the Network Mask field, enter 255.255.255.255 if it is a single IP address, or enter the netmask if it is a network.

Note To reset the form, click **Reset**.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1159
Fls:
3701
Doc:

Step 5 Click **OK**.

Note The sensor begins logging and creates a log file that can be viewed by selecting Monitoring > Logs > IP Logs > Archived. Logging continues until the address is removed from the IP Logging list. IP Logging slows down the performance of the sensor.

Note The IP logs are in a binary TCP dump format. To view the contents of the logs, download them to your desktop, and run a tool like Ethereal to view the logged packets. You can download Ethereal from the following website:
www.ethereal.com

Configuring Blocking

You can configure a sensor to block an attack by generating ACL rules for publication to a Cisco IOS router, or a Catalyst 6000 family switch, or by generating shun rules on a PIX Firewall.

This section includes the following procedures:

- Setting Up Blocking on the Sensor, page 94
- Blocking with Multiple Sensors, page 101
- Tracking Which Hosts/Networks Are Being Blocked, page 106
- Manual Blocking/Unblocking, page 107

Setting Up Blocking on the Sensor

You can configure your sensor to block an attack by generating ACL rules for publication to a Cisco IOS router, or a Catalyst 6000 family switch, or by generating shun rules on a PIX Firewall. That device is referred to as a blocking device.

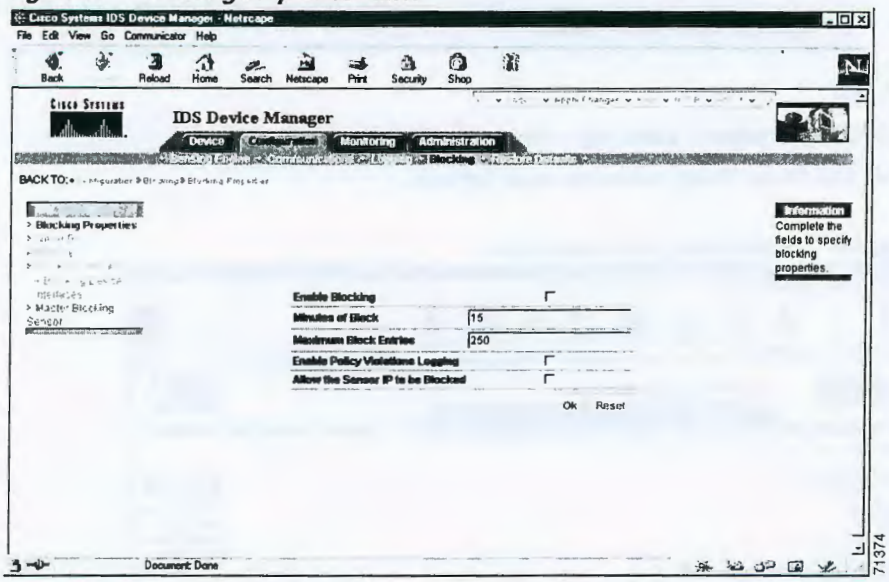
You must tune your sensor to identify hosts and networks that should never be blocked. You may have a trusted network device whose normal, expected behavior appears to be an attack. But such a device should never be blocked. And trusted, internal networks should never be blocked. Proper tuning of signatures reduces the number of false positives and helps ensure proper network operation. Tuning and filtering of signatures prevents the alarms from being generated. If the alarm is not generated, the associated block also does not occur.

To set up blocking on the sensor, follow these steps:

Step 1 In the IDS Device Manager main window, select **Configuration > Blocking > Blocking Properties**.

Step 2 Result: The Blocking Properties panel appears.

Figure 74 Blocking Properties Panel



Step 3 Select the **Enable Blocking** check box to turn blocking on for the sensor.

Step 4 In the Minutes of Block field, enter the number of minutes you want an address to be blocked (1 to 32,767).

Default: 15

Step 5 In the Maximum Block Entries field, enter how many blocks are to be maintained simultaneously (0 to 1000).

Default: 250

Note The number of blocks will not exceed the Maximum Block Entries. If the maximum is reached, new blocks will not occur until existing blocks time out and are removed.

Step 6 Select the **Enable Policy Violations Logging** check box to enable the logging of ACL policy violations on the blocking device (optional).

Note To generate alarms for policy violations, configure a policy violation signature by selecting Configuration > Sensing Engine > ACL Policy Violations. See the "Configuring IDS-Defined ACLs" section on page 70 for more information.

Default: Not selected

Step 7 Do not select the **Allow the Sensor IP to be Blocked** check box unless necessary.

Caution We recommend that you do not allow the sensor to block itself, because it will stop communicating with the managed device. If you can ensure that sensor creating a rule to block its own IP address will not prevent the sensor from accessing the blocking device, you can select this option.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1160
3701
Doc:

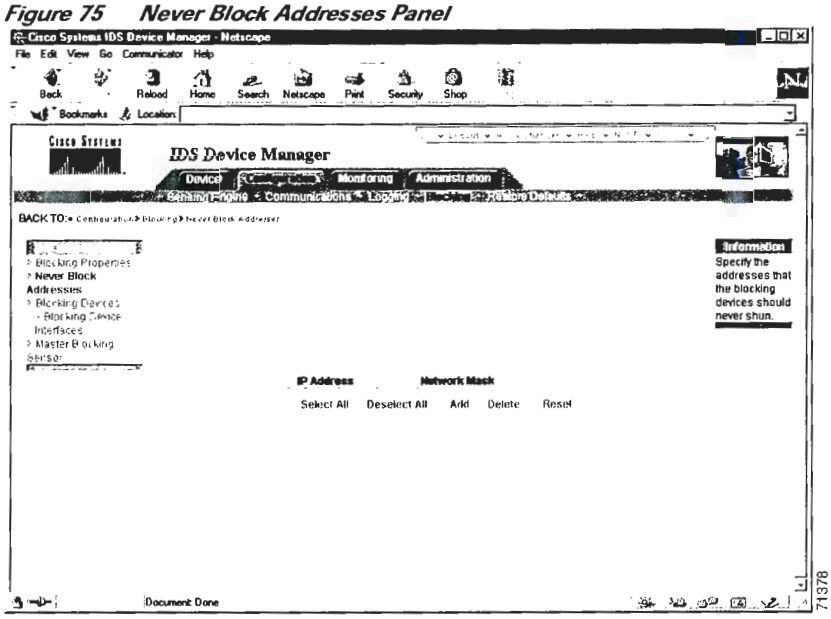
Note To reset the form, click **Reset**.

Step 8 Click **OK**.

Step 9 Select **Configuration > Blocking > Never Block Addresses**.

Result: The Never Block Addresses panel appears.

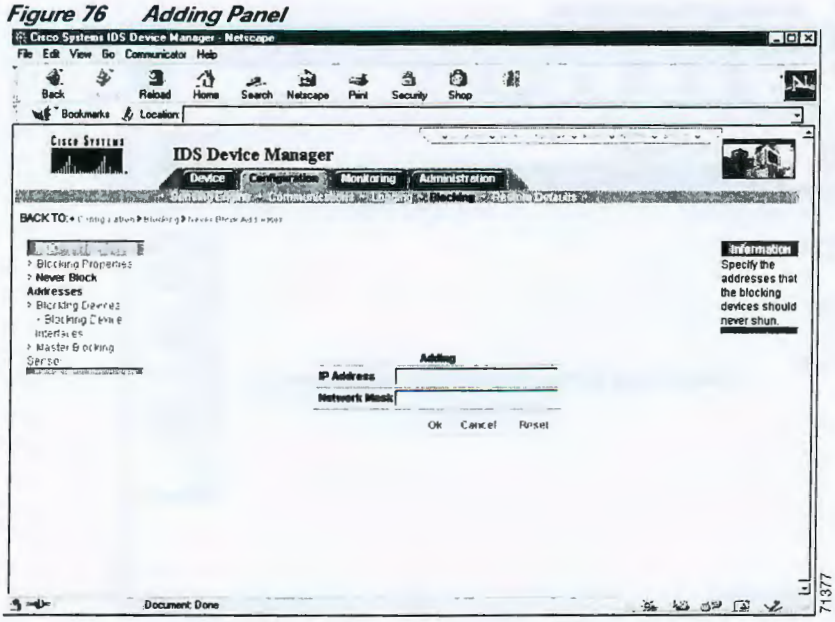
Figure 75 Never Block Addresses Panel



Step 10 Click **Add** to add addresses the blocking devices should never block.

Step 11 Result: The Adding panel appears.

Figure 76 Adding Panel



Step 12 In the IP Address field, enter the IP address of the host or network that should never be blocked.

Step 13 In the Network Mask field, enter 255.255.255.255 if it is a host, or enter the network mask of the network that should never be blocked.

Note To reset the form, click **Reset**.

Step 14 Click **OK**.

Step 15 Select **Configuration > Blocking > Blocking Devices**.

Result: The Blocking Devices panel appears.

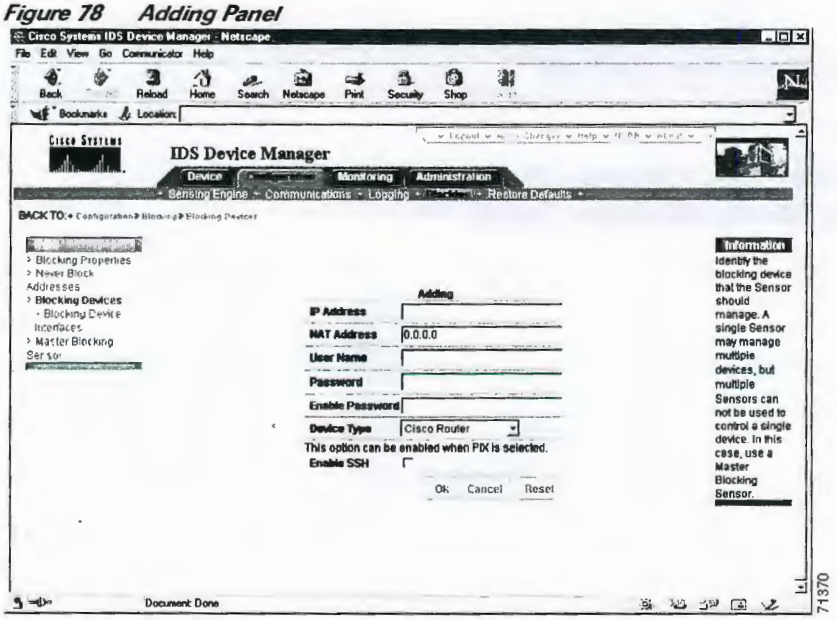
RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1161
3701
Doc:

Figure 77 Blocking Devices Panel

Step 16 Click **Add** to add the blocking devices that the sensor will manage.

Step 17 Result: The Adding panel appears.

Figure 78 Adding Panel



Caution A single sensor can manage multiple devices, but multiple sensors cannot be used to control a single device. In this case, use a master blocking sensor. See the "Blocking with Multiple Sensors" section on page 101 for the procedure for setting up a master blocking sensor.

Step 18 In the IP Address field, enter the address of the blocking device.

4.109

Step 19 In the NAT Address field, enter the NAT address of the sensor.

Note This is only necessary when the sensor is connecting to the managed device through another router or firewall that is using NAT translation of the IP address of the sensor. In this case, enter the IP address that the IP address of the sensor is being translated to.

Step 20 In the User Name field, enter the user that Telnets to the blocking device (1 to 16 characters).

Note The user name is optional if no user name is needed to log on to the device.

Step 21 In the Password field, enter the Telnet or SSH password of the blocking device (1 to 16 characters).

Step 22 In the Enable Password field, enter the enable password of the blocking device (1 to 16 characters).

Note The enable password is optional if the user already has enable privileges.

Step 23 In the Device Type field, enter the type of device that will do the blocking (Cisco Router, Catalyst 6000 VACL, PIX).

Step 24 Select the **SSH** check box, if PIX is the Device Type.

Note To reset the form, click **Reset**.

Step 25 Click **OK**.

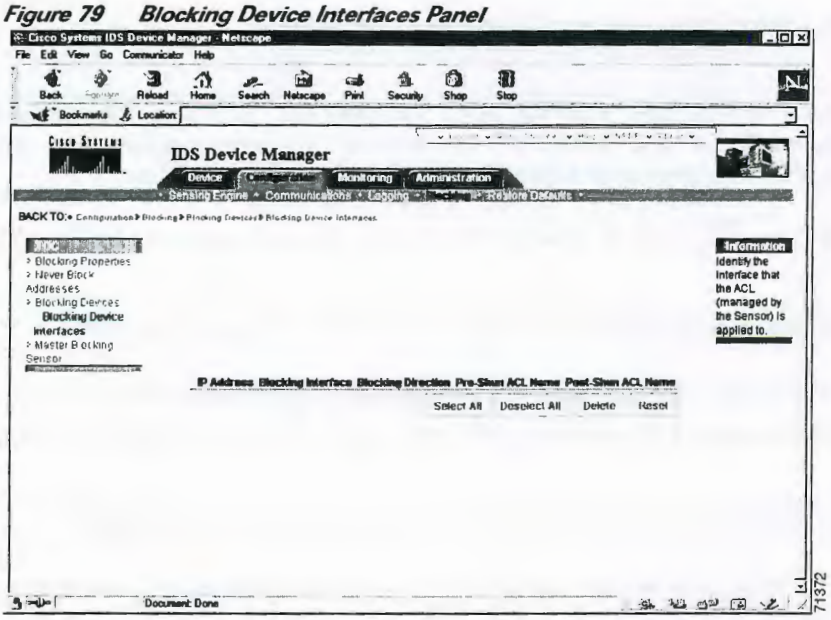
Note You do not have to designate an interface for the PIX Firewall. If you are using a PIX Firewall, the procedure is complete. You must designate at least one interface for all other devices.

Step 26 Select **Configuration > Blocking > Blocking Device Interfaces**.

Result: The Blocking Device Interfaces panel appears.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1162
3701
Doc:

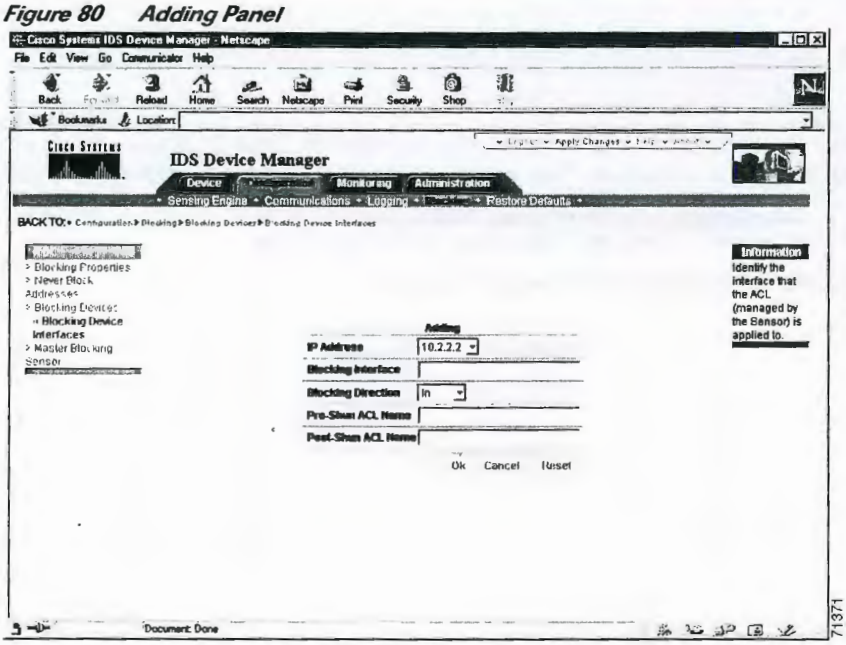
Figure 79 Blocking Device Interfaces Panel



Step 27 Click **Add** to configure the interfaces for each blocking device.

Result: The Adding panel appears.

Figure 80 Adding Panel



Note You cannot configure the interfaces for the PIX Firewall. The blocking direction is not available for Catalyst 6000 VACL devices.

Step 28 In the IP Address field, enter the address of the blocking device.

Step 29 I n the Blocking Interface field, enter the interface on the blocking device that is used for blocking (1 to 32 characters).

Note If you are using Catalyst 6000 family VACLS for blocking, enter the VLAN number.

Step 30 From the Blocking Direction list box, select the direction of the traffic flowing through the interface that should be blocked (in, out).

Step 31 In the Pre Shun ACL Name field, enter the name of the preblock ACL (1 to 64 characters).

Step 32 In the Post Shun ACL Name field, enter the name of the postblock ACL (1 to 64 characters).

Note To reset the form, click **Reset**.

Step 33 Click **OK**.

Note For more information on preshun and postshun ACLS, refer to the *Cisco Intrusion Detection System Sensor Configuration Note Version 3.1* found at the following website: http://www.cisco.com/univercd/cc/td/doc/product/iaabu/csids/csids8/index.htm

Blocking with Multiple Sensors

Multiple sensors can forward blocking requests to a specified master blocking sensor, which controls one or more devices. The sensor that is sending its block requests to the master blocking sensor is referred to as a "blocking forwarding sensor." On the blocking forwarding sensor, you must specify which remote host serves as the master blocking sensor. And on the master blocking sensor you must add the blocking forwarding sensors to its remote host configuration.

Note When using a master blocking sensor only the master blocking sensor is configured to manage the network devices. The blocking forwarding sensors should not be configured to manage network devices.

This section includes these topics:

- Configuring the Master Blocking Sensor, page 101
- Configuring the Blocking Forwarding Sensor, page 103

Configuring the Master Blocking Sensor

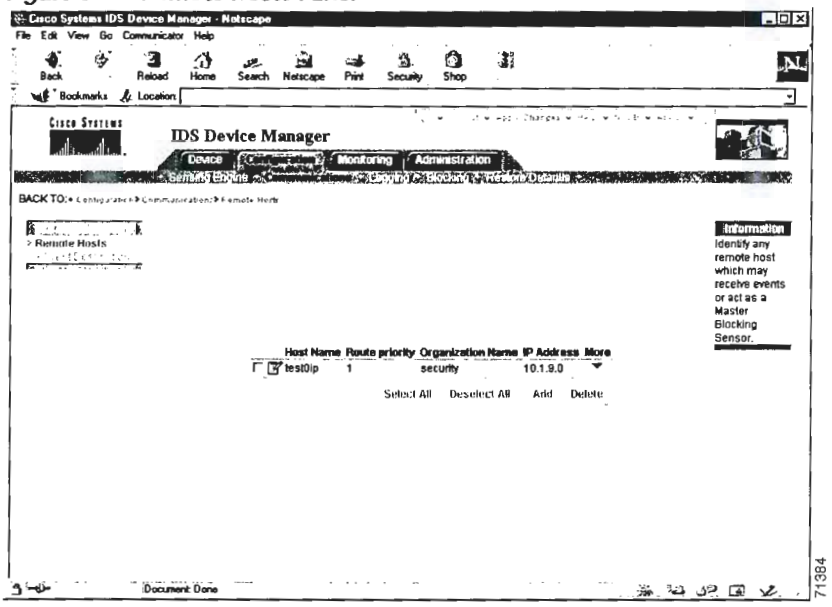
To configure the master blocking sensor, follow these steps:

Step 1 In the IDS Device Manager main window, select **Configuration > Communications > Remote Hosts**.

Result: The Remote Hosts panel appears.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1163
3701
Doc:

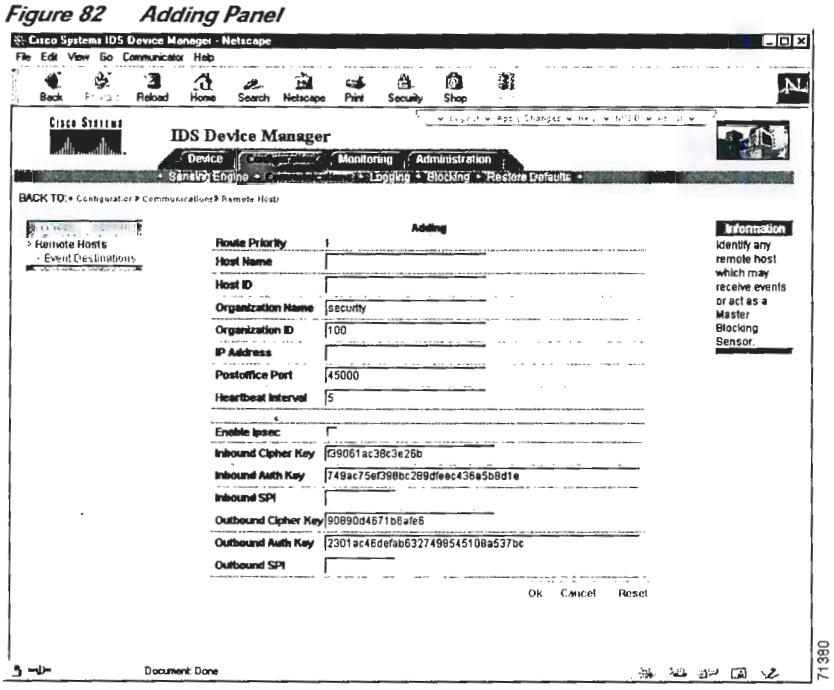
Figure 81 Remote Hosts Panel



Step 2 Click **Add** to add a remote sensor as a blocking forwarding sensor.

Result: The Adding panel appears.

Figure 82 Adding Panel



Step 3 In the Host Name field, enter the name of the blocking forwarding sensor (1 to 256 characters).

Step 4 In the Host ID field, enter the Host ID of the blocking forwarding sensor (1 to 65535).

Step 5 In the Organization Name field, enter the organization name of the blocking forwarding sensor (1 to 256 characters).

Step 6 In the Organization ID field, enter the organization ID of the blocking forwarding sensor (1 to 65535).

Step 7 In the IP Address field, enter the IP address of the blocking forwarding sensor.

Step 8 In the Post Office Port field, enter the Post Office port on the blocking forwarding sensor (1025 to 65535).

Default: 45000

Step 9 In the Heartbeat Interval field, enter the remote Post Office heartbeat interval (1 to 65535).

Default: 5

Step 10 Do not select the **Enable IPSec** check box for the blocking forwarding sensor.

Default: Off

Note You can enable IPSec on the remote host if you are using the Cisco IDS Director or the Cisco Security Policy Manager rather than the IDS Device Manager as your IDS manager. Refer to your IDS manager documentation for the procedure for configuring IPSec. If you want to configure IPSec between two sensors, for instance, between the master blocking sensor and the blocking forwarding sensor, refer to the *Cisco Intrusion Detection System Sensor Configuration Note Version 3.1* for the instructions. The configuration note is found at the following website: http://www.cisco.com/univercd/cc/td/doc/product/iaabu/csids/csids8/index.htm

Note To reset the form, click **Reset**.

Step 11 Click **OK**.

Note Repeat these steps for each blocking forwarding sensor you need to add to the master blocking sensor.

Configuring the Blocking Forwarding Sensor

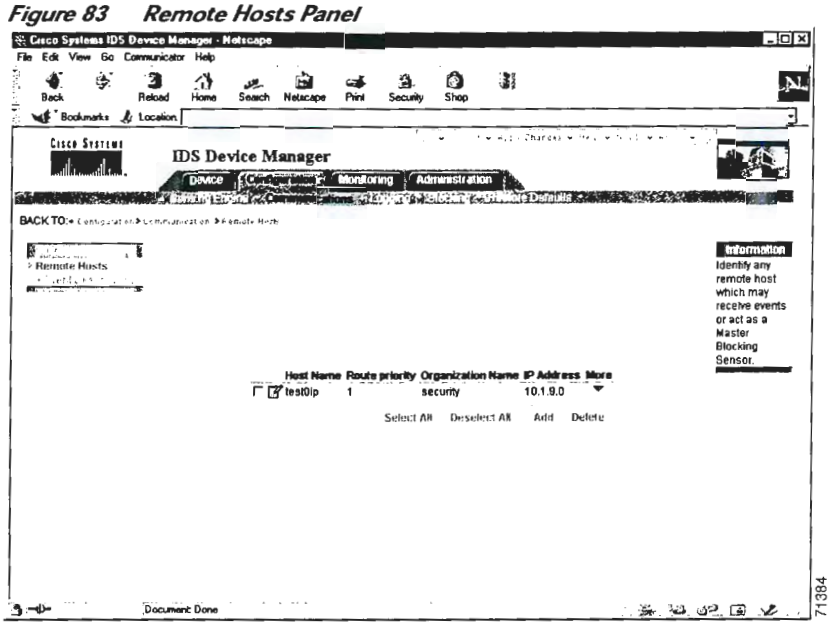
To configure a blocking forwarding sensor, follow these steps:

Step 1 In the IDS Device Manager main window, select **Configuration** > **Communications** > **Remote Hosts**.

Result: The Remote Hosts panel appears.

RQS Nº 03/2005 - CN - CPMI - CORREIOS
1164
Fls:
3701
Doc:

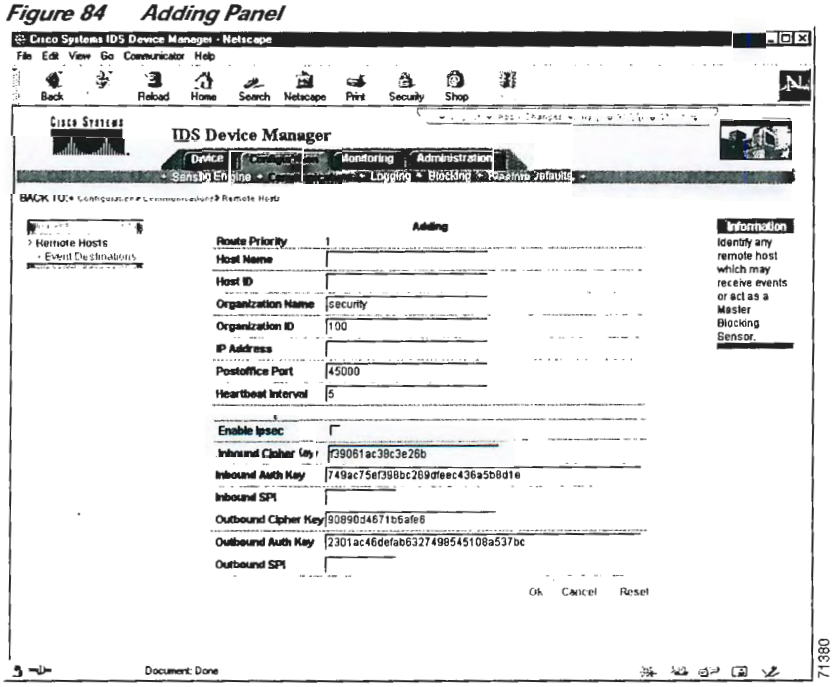
Figure 83 Remote Hosts Panel



Step 2 Click **Add** to add a remote sensor as a master blocking sensor.

Result: The Adding panel appears.

Figure 84 Adding Panel



Step 3 In the Host Name field, enter the name of the master blocking sensor (1 to 256 characters).

Step 4 In the Host ID field, enter the host ID of the master blocking sensor (1 to 65535).

Step 5 In the Organization Name field, enter the organization name of the master blocking sensor (1 to 256 characters).

Step 6 In the Organization ID field, enter the organization ID of the master blocking sensor (1 to 65535).

Step 7 In the IP Address field, enter the IP address of the master blocking sensor.

Step 8 In the Post Office Port field, enter the Post Office port on the master blocking sensor (1025 to 65535).

Default: 45000

Step 9 In the Heartbeat Interval field, enter the remote Post Office heartbeat interval (1 to 65535).

Default: 5

Step 10 Do not select the **Enable IPSec** check box for the master blocking sensor.

Default: Off

Note You should only enable IPSec on the remote host if you are using the Cisco IDS Director or CSPM rather than the IDS Device Manager as your IDS manager.

Note To reset the form, click **Reset**.

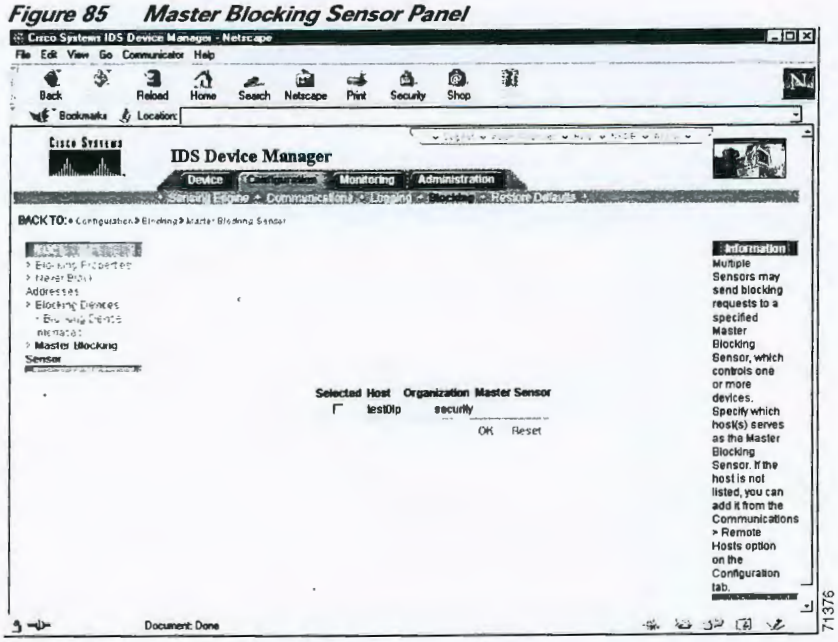
Step 11 Click **OK**.

Result: The remote host is added to both the Remote Hosts and the Master Blocking Sensor panels.

Step 12 In the IDS Device Manager main window, select **Configuration > Blocking > Master Blocking Sensor**.

Result: The Master Blocking Sensor panel appears.

Figure 85 Master Blocking Sensor Panel



Step 13 Select the hosts check box that you want to be master blocking sensors.

ROS Nº 03/2005 - CPI
CPMI - CORREIOS
Fls: 1165
Doc: 3701

Step 14 Click **Enable**.

Note To reset the form, click **Reset**.

Step 15 Click **OK**.

Note Repeat this procedure on each blocking forwarding sensor.

Tracking Which Hosts/Networks Are Being Blocked

On occasion, you may want to determine which addresses are being blocked. You can see the list of addresses and networks on the Manual Blocking panel. This panel also shows you the current status of devices, which are being managed by the sensor.

To view the list of addresses and networks being blocked, follow these steps:

Step 1 In the IDS Device Manager main windows, select **Administration** > **Manual Blocking**.

Result: The Manual Blocking panel appears

Figure 86 Manual Blocking Panel

You can see a list of all host/network addresses being blocked and the current status of devices.

Manual Blocking/Unblocking

On occasion, you may want to block an address for a short period of time. You can configure the address and the amount of time on the Manual Blocking panel.

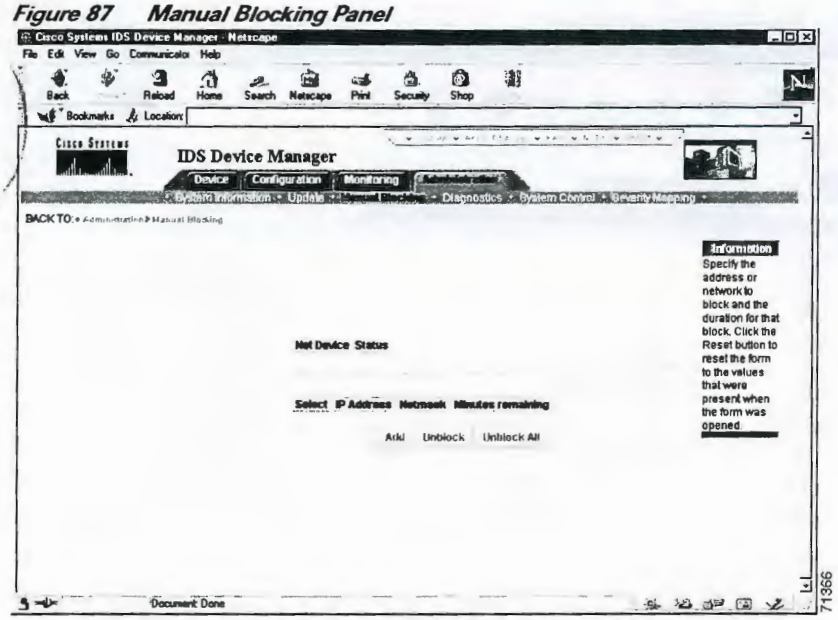
To configure manual blocking, follow these steps:

Step 1 In the IDS Device Manager main windows, select **Administration > Manual Blocking**.

Result: The Manual Blocking panel appears.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1166
Doc: 3701

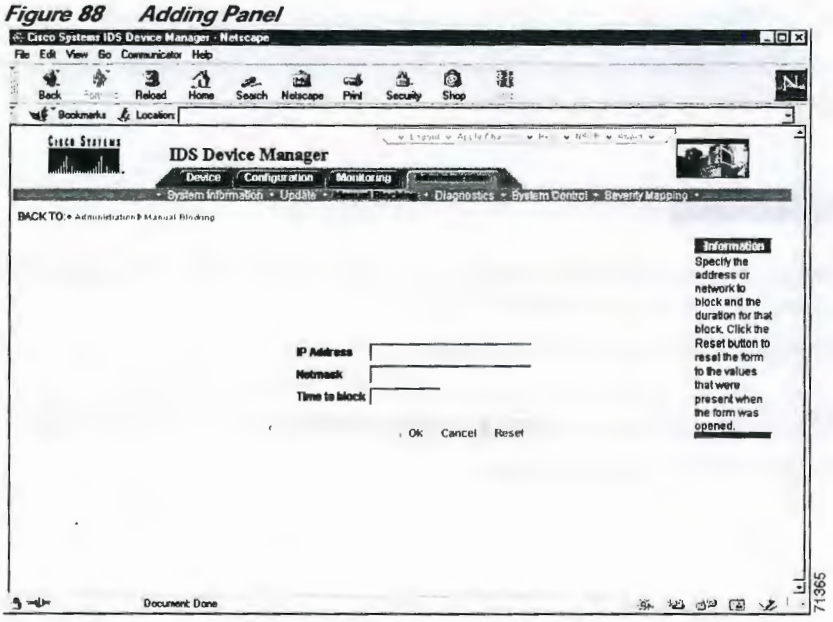
Figure 87 Manual Blocking Panel



Step 2 Click **Add** to add an address.

Result: The Adding panel appears.

Figure 88 Adding Panel



Step 3 In the IP Address field, enter the IP address to be blocked.

Caution If you are blocking a single IP address, leave the netmask field blank. Filling in the netmask prevents the IP address from being blocked on a PIX Firewall.

4.099

Note PIX Firewalls do not block networks.

Step 4 In the Netmask field, enter the netmask address to be blocked.

Step 5 In the Time to block field, enter the number of minutes to block (1-70560).

Note Entering -1 creates a permanent block.

Note To reset the form, click **Reset**.

Step 6 Click **OK**.

Result: The Manual Blocking panel appears showing the minutes for the block. Click **Refresh** in your browser to see the minutes pass.

Figure 89 Monitoring Blocking Panel

Step 7 To cancel the block before the assigned minutes have passed, click **Unblock**.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1167
Doc: 3701

Monitoring Tasks

This section includes the following procedures:

- Log Files, page 110
- Viewing Log Files, page 112
- Viewing Sensing Interface Statistics, page 116
- Downloading the IDS Event Viewer, page 117

Log Files

This section includes the following topics:

- Event Logs, page 110
- Error and Command Logs, page 111
- IP Session Logs, page 112

Event Logs

Event logs are ASCII files written to the /usr/nr/var directory with the naming convention of log.YYYYMMDDHHMM. Log files capture data on alarms, command, and errors.

Event alarm data are unique because the record format contains optional as well as fixed components.

Fixed alarm data include the following information:

- Which sensor detected the event.
- When the alarm was generated.
- The type of alarm.
- The source and target of the event.

The optional data field contains information that cannot be described by the fixed portion of the alarm record format. This information may be a string associated with an event, or context data that consists of a snapshot of incoming and outgoing TCP traffic (a 256-byte maximum in both directions).

Example 1 shows a typical line written to a log file.

Example 1 Log File Line

```
4,1025294,1998/04/16,16:58:36,1998/04/16,11:58:36,10008,11,100,OUT,OUT,1,2001,0,TCP/IP,
10.1.6.1,10.2.3.5,0,0,0.0.0.0,
```

Each comma-delimited field contains different data. The first field indicates what kind of record was logged. Table 1 maps the initial field of a log file with its corresponding record type.

Table 1 Log File Initial Field Reference Values

Field Values	Record Types
2	Error
3	Command Log
4	Event (alarm)

In the previous table, field value 4 denotes an event record. Table 2 provides a reference for the rest of the fields in Example 1.

Table 2 Log File Field Reference Values

Sample Field Value	Field Type
4	Record Type
1025294	Record ID
1998/04/16	GMT Datestamp
16:58:36	GMT Timestamp
1998/04/16	Local Datestamp
11:58:36	Local Timestamp
10008	Application ID
11	Host ID
100	Organization ID
OUT	Source Direction
OUT	Destination Direction
1	Alarm Level
2001	SigID
0	SubSigID
TCP/IP	Protocol
10.1.6.1	Source IP Address
10.2.3.5	Destination IP Address
0	Source Port
0	Destination Port
0.0.0.0	Router IP Address
phf	String Data
474554206A756E6B2F7068 663F6A756E6B0DZZ	Context Data[1]

1. The context data is encoded in a hexadecimal-ASCII format, which has two characters for each one represented, converted to hexadecimal. For example, the letter "A" is represented as 41. Context may contain bidirectional traffic, that is, both sides of a conversation. The separator for the two sides of the context is the two characters is "ZZ."

Error and Command Logs

Two other types of records, error and command log, are similar in structure to the event record. Both of these record types have the same first eight fields contained in event records (Record Type, Record ID, GMT Date and Timestamp, Local Date and Timestamp, Application ID, Host ID, and Organization ID).

RQS Nº 05/2005 - CN
CPMI - CORREIOS
1168
Fls:
3701
Doc:

An error record type has a ninth field denoting the actual error string generated by a service. The command log record type also contains fields for the source application ID, host ID, and organization ID, in addition to the command string. In both cases, you have a complete record of errors and commands.

Errors are also written to error files specific to each daemon.

IP Session Logs

IP session logs capture all incoming and outgoing TCP packets associated with a specific IP address, and therefore contain binary data. They are written to a /usr/nr/var/iplog directory of the sensor with the naming convention of iplog.source_IP_address.yyyymmddhhmm.

In addition to detecting attack signatures, *packetd* is able to monitor the traffic associated with a specific type of attack. For example, *packetd* can be configured to monitor all packets associated with an IP spoof. The *packetd* daemon creates a separate log file in /usr/nr/var/iplog for each of these monitoring sessions. The name of each session log file is based on the IP address of the attacking host and a time stamp (for example, iplog.10.145.16.152.yyyymmddhhmm). When the IP log file is closed, it is moved to the /usr/nr/var/iplog/new directory.

Viewing Log Files

Log files are stored in the following directories:

- Event logs are stored in the /usr/nr/var directory.
- IP logs are stored in the /usr/nr/var/iplog directory.
- Error logs are stored in the /usr/nr/var/errors directory.

To view and save log files, follow these steps:

Step 1 In the IDS Device Manager main windows, select **Monitoring > Logs > Events > Current**.

Result: The Current panel appears.

Figure 90 Current Panel

Step 2 Click the file name to view the log file.

Result: The log file appears on another browser page if the file is not empty.

Note All log files start out as a certain size and are then filled with data. The percentage used designates the percent of a log file that has been written to so far.

Note If the log file is empty, the browser prompts you to save the file because it cannot open it.

Note You can click the column headers to sort up and down.

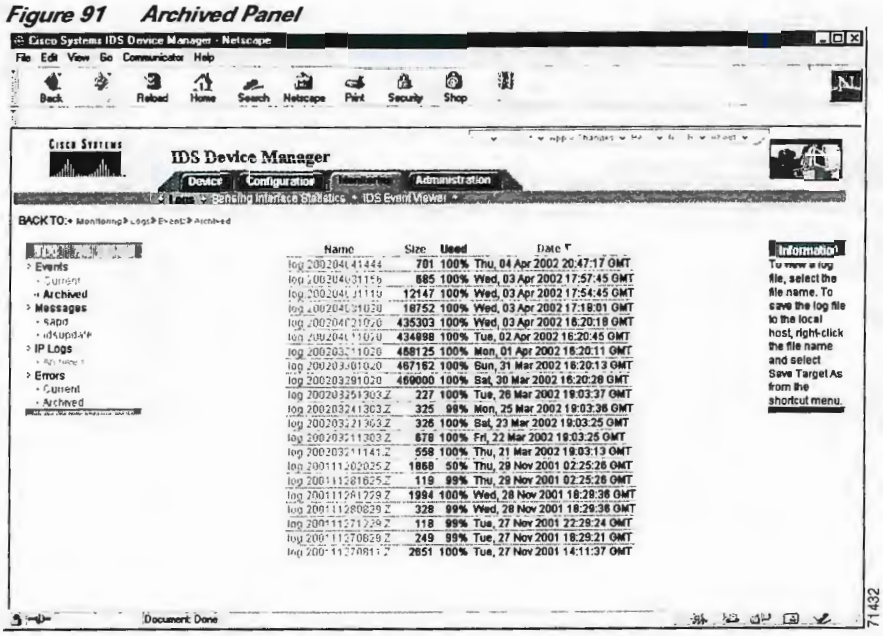
Step 3 To save the log file, select **File > Save As** in your browser.

Step 4 To view archived logs, select **Monitoring > Logs > Events > Archived**.

Result: The Archived panel appears.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1169
Fls:
3701
Doc:

Figure 91 Archived Panel



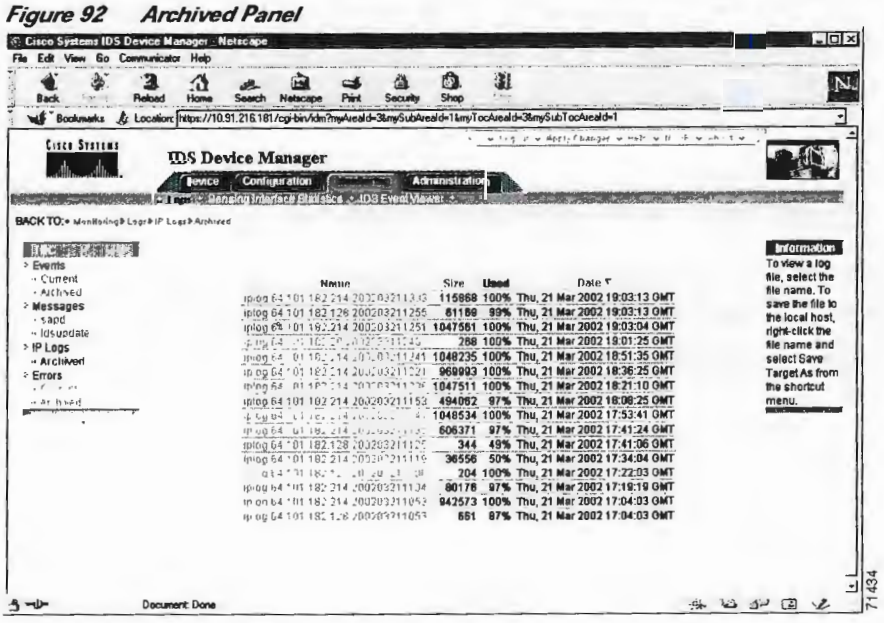
Step 5 Click any file to view the archived event logs.

Result: The archived event log appears in a new page of your browser.

Step 6 Select **Monitoring > Logs > IP Logs > Archived** to display archived IP logs.

Result: The Archived panel appears.

Figure 92 Archived Panel



Step 7 Select **File > Save As** in your browser to download the IP log file.

4093

Caution Some web browsers download the file in the ASCII format rather than in a binary format. The IP log must be downloaded in a binary format.

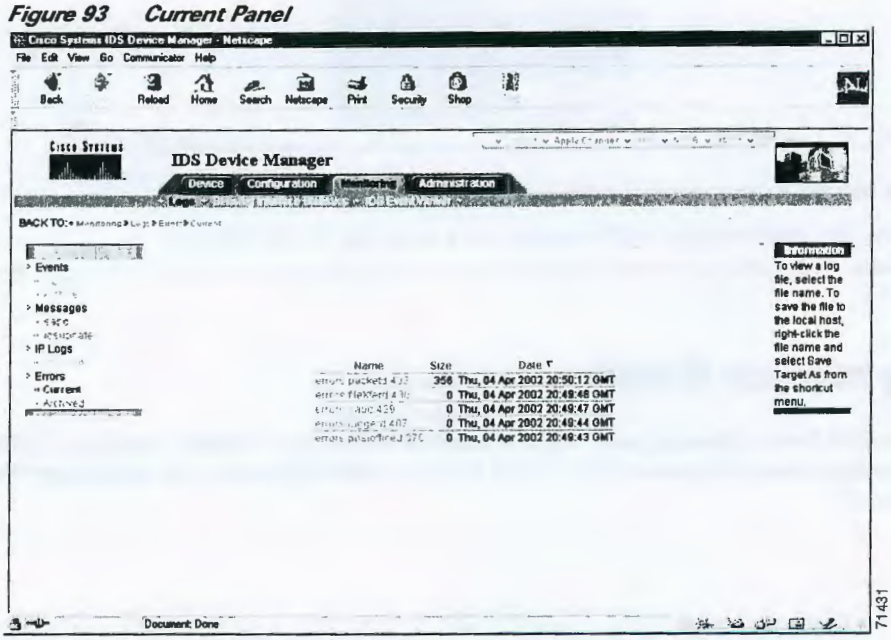
Note The IP logs are in a binary TCP dump format. To view the contents of the logs, download them to your desktop, and run a tool like Ethereal to view the logged packets. You can download Ethereal from the following website:
www.ethereal.com

Step 8 Select **Monitoring > Logs > Errors > Current** to display the current error logs.

The error logs contain informational messages and error messages.

Result: The Current panel appears.

Figure 93 Current Panel



Step 9 Click any file name to view the error logs for the daemons currently running.

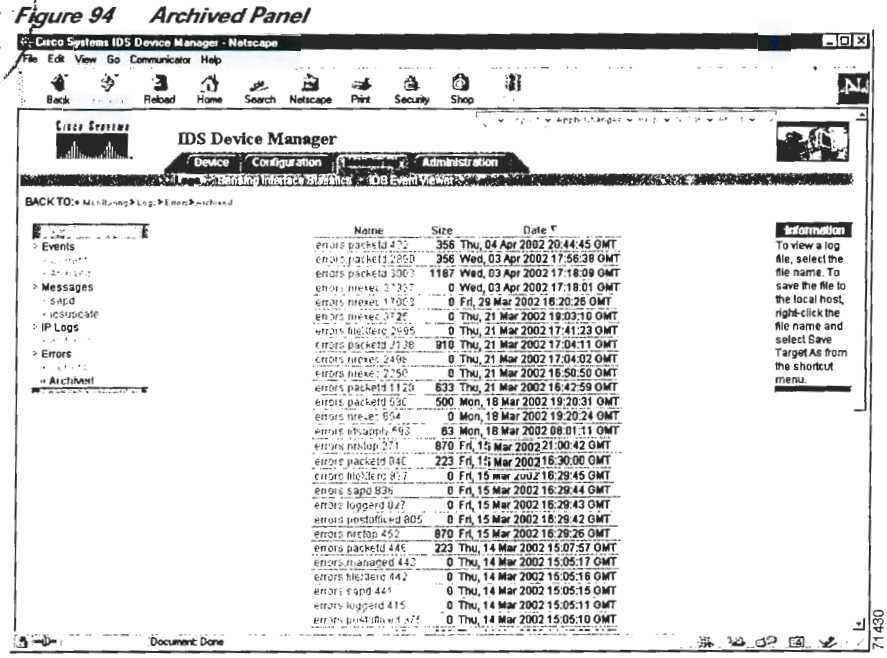
Result: The current error log file appears in a new page of your browser.

Step 10 Select **Monitoring > Logs > Errors > Archived** to display the error logs stored in the /usr/nr/var/errors directory.

Result: The Archived panel appears.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1170
Doc: 3701

Figure 94 Archived Panel



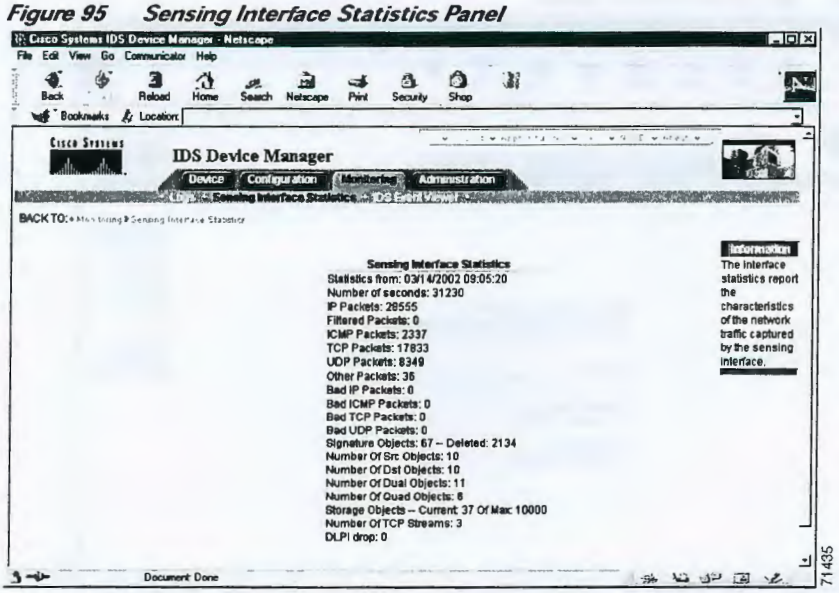
Step 11 Click any file name to view the archived error log files.

Result: The archived error log file appears in a new page of your browser.

Viewing Sensing Interface Statistics

In the IDS Device Manager main window, select **Monitoring > Sensing Interface Statistics** to view a report that shows the characteristics of the network traffic captured by the sensing interface (see Figure 95):

Figure 95 Sensing Interface Statistics Panel



You can use the Sensing Interface Statistics panel to verify that the sensing interface is seeing traffic. If the IP packets and other counters are set to zero, the sensor is not detecting traffic. If the sensor is not detecting traffic, refer to the "Troubleshooting" section in *Cisco Intrusion Detection System Getting Started Version 3.1* found at the following website for more information:

http://www.cisco.com/univercd/cc/td/doc/product/iaabu/csids/csids8/index.htm

Downloading the IDS Event Viewer

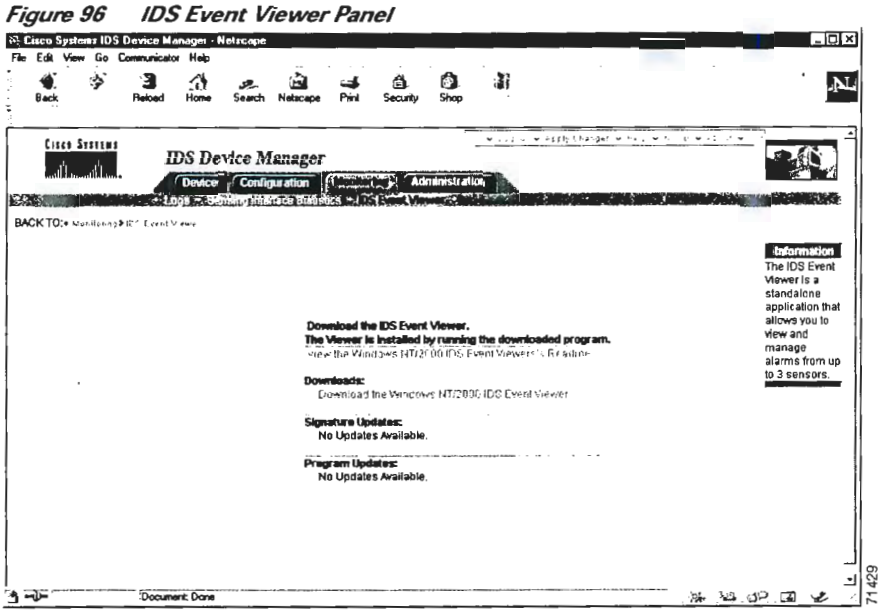
To download the IDS Event Viewer, follow these steps:

Step 1 In the IDS Device Managermain window, select **Monitoring > IDS Event Viewer**.

Result: The IDS Event Viewer panel appears.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1171
Doc: 3701

Figure 96 IDS Event Viewer Panel



Step 2 Click **View the Event Viewer's Readme** to see information on installation, running the IDS Event Viewer, and signatures.

Step 3 Click **Download the Windows NT/2000 IDS Event Viewer** to install the IDS Event Viewer.

Step 4 Copy the executable to the directory of your choice.

Step 5 Install the IDS Event Viewer.

For installation instructions, refer to *Cisco Intrusion Detection System Getting Started Version 3.1* or the *Cisco Intrusion Detection System Event Viewer Configuration Note Version 3.1* found at the following website:
http://www.cisco.com/univercd/cc/td/doc/product/iaabu/csids/csids8/index.htm

Note You can use the IDS Event Viewer to manage up to three sensors.

For more detailed information on configuring and using the IDS Event Viewer, refer to the *Cisco Intrusion Detection System Event Viewer Configuration Note Version 3.1* found at the following website:

http://www.cisco.com/univercd/cc/td/doc/product/iaabu/csids/csids8/index.htm

Administrative Tasks

This section includes the following topics:

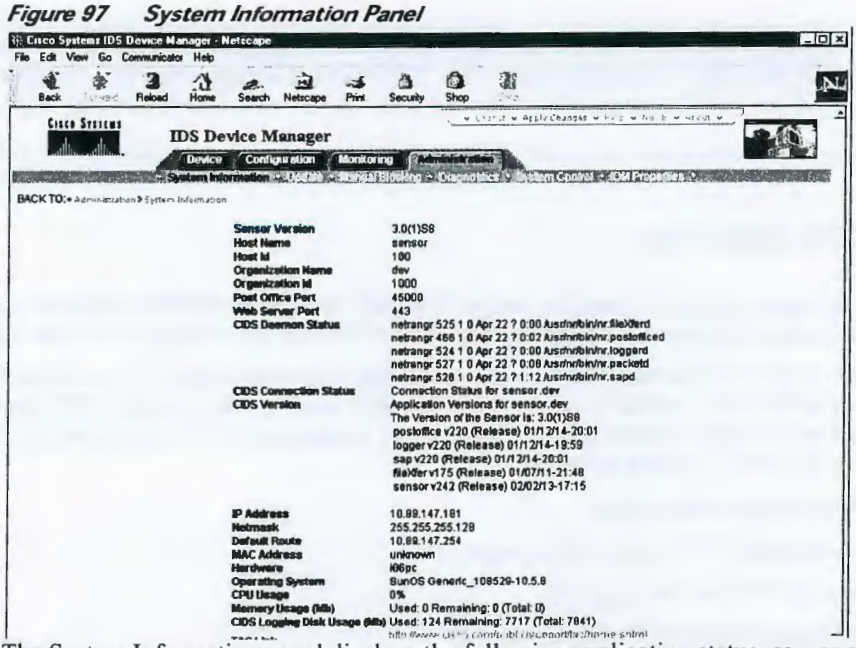
- Viewing System Information, page 119
- Configuring Automatic Updates, page 120
- Running and Viewing Diagnostics, page 122

- Starting and Stopping Processes, page 123
- Setting Up Severity Levels, page 124

Viewing System Information

You can view your system information by selecting **Administration > System Information** in the IDS Device Manager main window (see Figure 97).

Figure 97 System Information Panel



The System Information panel displays the following application status, sensor appliance, and support information:

- Sensor Version
- Host Name
- Host ID
- Organization Name
- Organization ID
- Post Office Port
- Web Server Port
- IP Address
- Netmask
- Default Route
- CSIDS Daemon Status—Displays all the daemons that are running
- CSIDS Connection Status—Displays the Postoffice connection status with remote destinations and connection status with managed devices.
- CSIDS Version—Displays the version of the running daemons

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1172
Doc: 3701

- MAC Address
- Hardware
- Operating System
- CPU usage
- Memory usage (MB)
- CSIDS Logging Disk Space Usage (MB)
- TAC link

Note From this panel, you can tell whether the sensor is communicating with the IDS Event Viewer by what is listed under the CIDS Connection Status line. [Established] indicates that the connection is viable. [SynSent] indicates that the connection is down and the sensor is not communicating with the IDS Event Viewer.

Configuring Automatic Updates

You can configure automatic signature and service pack updates, so that when signatures or service packs are loaded on a central FTP server, they will be downloaded and applied to your sensor.

If the FTP server or the network between the sensor and the server is slow, it is possible for an FTP file transfer timeout for the update to occur. The update FTP session times out after 600 seconds. If this occurs, an error is logged in the errors.idsapply.txt or idsapply.txt if IDS is not running. The update is not attempted when a timeout occurs.

This section includes these topics:

- Increasing the FTP Timeout Value, page 120
- Supported FTP Servers, page 121
- Configuring Automatic Updates, page 121

Increasing the FTP Timeout Value

To increase the timeout, follow these steps:

Step 1 Log in to the sensor as root.

Step 2 Type the following:

```
SAP_FTP_TIMEOUT=1200
export SAP_FTP_TIMEOUT
```

Step 3 Type the following:

```
/usr/nr/bin/idsupdate stop
```

Step 4 Type `idsupdate` to reschedule the updates.

Result: The new updates use 1200 seconds as the FTP timeout value.

Supported FTP Servers

The following FTP servers are supported for updates:

- Sambar FTP Server Version 5.0 (win32)
- Web-mail Microsoft FTP Service Version 5.0 (win32)
- Serv-U FTP-Server v2.5h for WinSock (win32)
- Solaris 2.8
- HP-UX (HP-UX qdir-5 B.10.20 A 9000/715)
- Windows 2000 (Microsoft ftp server version 5.0)
- Windows NT 4.0 (Microsoft ftp server version 3.0)

Note The sensor cannot automatically download signature update and service packs from Cisco.com. You need to download the signature update or service pack to your own FTP server, and then configure the sensor to download them from your FTP server.

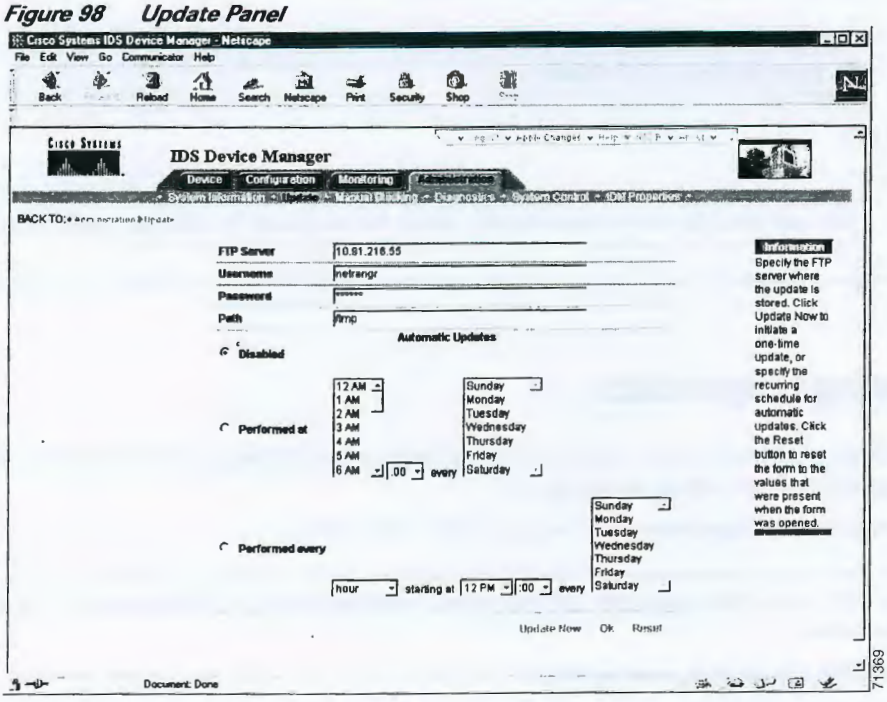
Configuring Automatic Updates

To configure automatic signature and service pack updates, follow these steps:

Step 1 In the IDS Device Manager main window, select **Administration > Update**.

Result: The Update panel appears.

Figure 98 Update Panel



Step 2 In the FTP Server field, enter the IP address of the FTP server to poll for updates.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1173
Fls:
3701
Doc:

Note The sensor does not use DNS so you must enter the IP address and not the name.

Step 3 In the Username field, enter the username to use when logging into the FTP server (1 to 16 characters).

Step 4 In the Password field, enter the username password on the FTP server (1 to 16 characters).

Step 5 In the Path field, enter the path to the directory on the FTP server where the updates are located (1 to 128 characters).

Note The path entered is relative to the directory where you log in. To use an absolute path, add an extra "/" before the directory name.

Step 6 Perform one of the following:

- Select the **Disabled** check box.
- Select the **Performed at** check box.

  Specify the specific times the update mechanism should run by selecting a time and day from the list boxes.

Note You can select multiple times and days. Select times when there is little user activity on the network.

- Select the **Performed every** check box.

  Schedule recurring updates by selecting an hour, time, and day from the list boxes.
- Click **Update Now** to apply the update immediately.

Note To reset the form, click **Reset**.

Step 7 Click **OK**.

Note You can have the sensor immediately check for an update by clicking Update Now.

Running and Viewing Diagnostics

The diagnostics are designed to be used by TAC when troubleshooting a problem on the sensor. Prepare a diagnostics report before contacting TAC.

To run and view diagnostics on the sensor, follow these steps:

Step 1 In the IDS Device Manager main window, select **Administration** > **Diagnostics** in to run diagnostics on the sensor.

Result: The Diagnostics panel appears.

Figure 99 Diagnostics Panel

Step 2 Click **Run Diagnostics** to start the hardware diagnostics

Result: The results are displayed in a report, which includes a list of the installed OS packages.

Warning **This will run diagnostics on the sensor. The command may take several minutes to complete execution.**

Note Every time you click **Run Diagnostics**, you generate a new report.

Step 3 Click **View Last Report** to view the report that was generated the last time the diagnostics were run.

Note Running diagnostics on the sensor takes a while.

Step 4 To save the diagnostics report, select **Menu > Save As** in your browser.

Starting and Stopping Processes

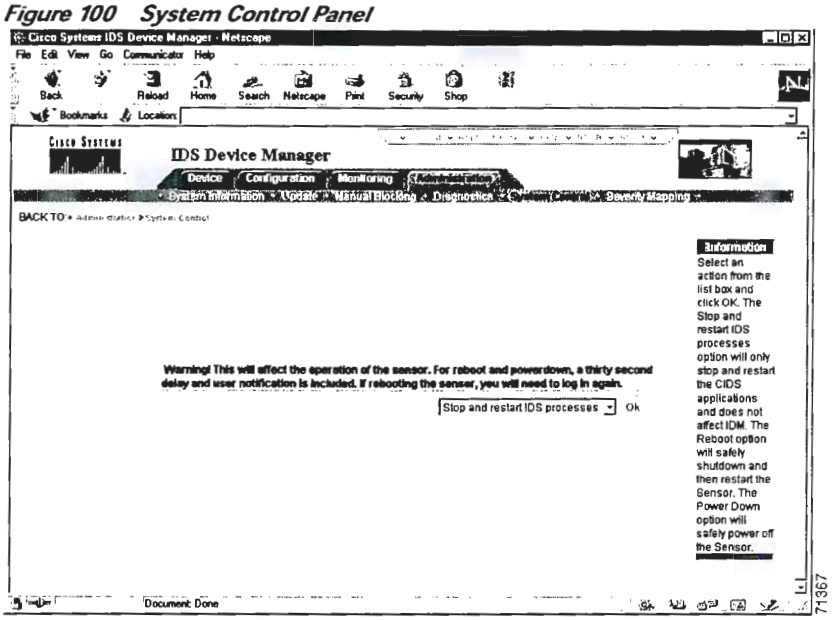
To stop and start IDS Device Manager processes, follow these steps:

Step 1 In the IDS Device Manager main window, select **Administration > System Control**.

Result: The System Control panel appears.

ROS Nº 03/2095 - CN
CPMI - CORREIOS
Fls: 1174
Doc: 3701

Figure 100 System Control Panel



Step 2 Select one of the following actions from the list box:

- Stop and restart IDS processes

  Stop and restart IDS processes only stops and restarts the IDS applications and does not affect the IDS Device Manager.

- Reboot

  Reboot safely shuts down and then restarts the sensor.

- Power Down

  Power Down safely powers off the sensor.

Warning **These actions affect the operation of the sensor. For reboot and power down, a thirty-second delay and user notification are included. If you reboot the sensor, you must log in to the IDS Device Manager after the sensor comes online.**

Step 3 Click **OK**.

Setting Up Severity Levels

You can assign text-based severity levels to Levels 1 though 5. Instead of displaying the numerical value of a severity, you see the text mapping as shown in the following default severity levels:

- 0 = None
- 1 = Information

  Information refers to events that on their own are not considered security relevant, but when combined with other information could be used to develop trends or conduct forensic research. Information alarms are identified by a blue icon in the IDS Event Viewer.

- 2 = Information
- 3 = Low

  Low refers to unusual or suspicious traffic and overt reconnaissance; events that are in violation of the gray area of an RFC. Low alarms are identified by a yellow icon in the IDS Event Viewer.

- 4 = Medium

  Medium refers to denial of service of auto-recoverable services, network and/or service floods, stealth scans, and extremely suspicious traffic. Medium alarms are identified by an orange icon in the IDS Event Viewer.

- 5 = High

  High refers to denial of service that is not automatically recoverable, exploits that result in unauthorized access of any type, and obviously malicious RFC violations. High alarms are identified by a red icon in the IDS Event Viewer.

Note If you change the severity mappings in the IDS Device Manager, you need to also change the corresponding severity mappings in the IDS Event Viewer to maintain consistency.

To map severity levels, follow these steps:

Step 1 In the IDS Device Manager main window, select **Administration>IDM Properties>Severity Mapping**.

Result: The Severity Mapping panel appears.

Figure 101 Severity Mapping Panel

Step 2 Select one of the following values for each of the Level 1 though 5 fields:

- Information
- Low

RQS Nº 03/2005 - CN - CPMI - CORREIOS
1175
Fls:
Doc: 3701

- Medium
- High

Note The severity level must be equal to or greater than the severity level of the previous level. For example, Level 1 must be equal to or have a lower severity level than Level 2.

Note To reset the form, click **Reset**.

Step 3 Click **OK**.

Setting Signature Pagination

You can define the pagination properties for displaying signature pages, which affects the pagination for the lists under the following panels:

- Configuration > Sensing Engine > Signature Groups
- Configuration > Sensing Engine > Custom Signatures
- Configuration > Sensing Engine > TCP Connection Signatures
- Configuration > Sensing Engine > UDP Connection Signatures
- Configuration > Sensing Engine > String Signatures
- Configuration > Sensing Engine > ACL Policy Violations

To define signature pagination, follow these steps:

Step 1 In the IDS Device Manager main window, select **Administration > IDM Properties > Signature Pagination**.

Result: The Signature Pagination panel appears.

Figure 102 Signature Pagination Panel

Step 2 Select one of the following check boxes:

- Pagination Size—Enter the number of signature IDs to display on a page (5 to 1000).

  Default: 15
- Disabled

Note To reset the form, click **Reset**.

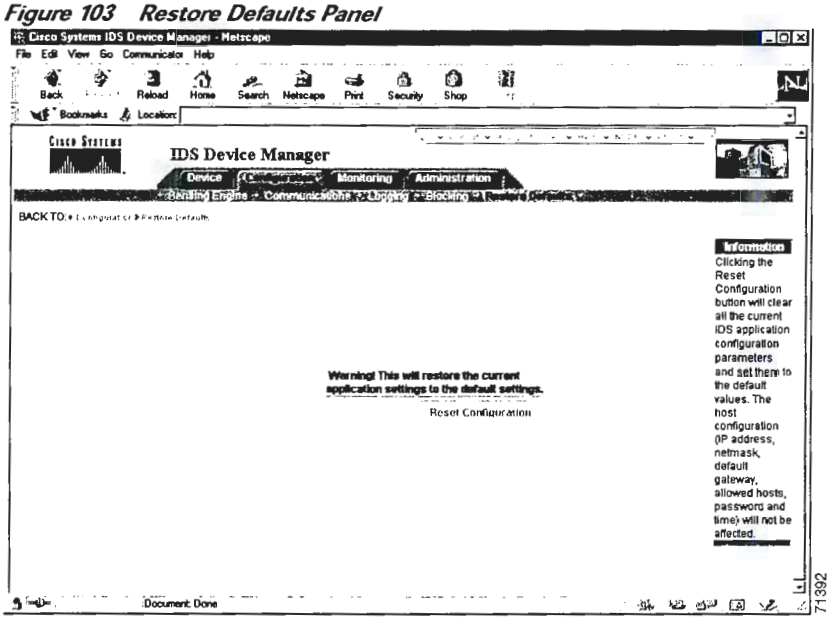
Step 3 Click **OK**.

Restoring Defaults

Select **Configuration > Restore Defaults** to clear all current configurations and restore the factory defaults to the sensor (see Figure 103).

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1176
Doc: 3701

Figure 103 Restore Defaults Panel



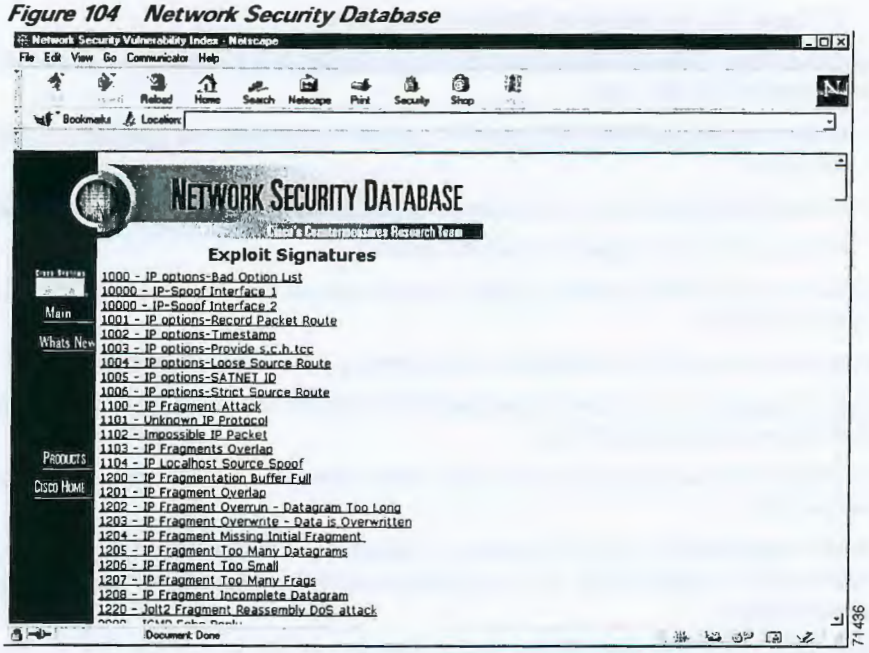
Caution Clicking Reset Configuration clears all the current IDS application configuration parameters and sets them to the default values. The host configuration (IP address, netmask, default gateway, allowed hosts, password, and time) are not affected.

4.079

Viewing the NSDB

Click **NSDB** on the ToolBar to view the Network Security Database (see Figure 104).

Figure 104 Network Security Database



A typical NSDB entry contains the following critical security information:

- Signature Name—The name of the signature appears at the top of the entry. In Figure 105, it is IP Fragment Incomplete Datagram.
- ID—A unique ID for the signature. In Figure 105, it is 1208.
- Sub ID—An optional subsignature ID for the signature. In Figure 105, it is 0, which means there is no subsignature ID.
- Recommended Alarm Level—The alarm level that we recommend you set for that signature. In Figure 105, it is 2.
- Signature Type—The signature type indicates what it affects.
  - Network—Categorizes a vulnerability as being network-based.
  - Host—Categorizes a vulnerability as being host-based.

Note Cisco IDS mainly uses the network classification because at this time no host-based signatures are being developed.

In Figure 105, the Signature Type is Network.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1177
Fls:
3701
Doc:

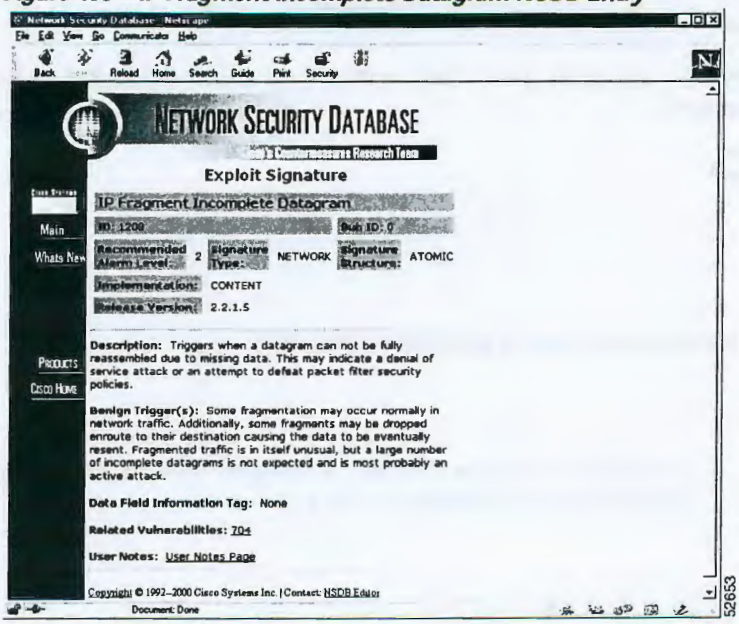
- Signature Structure—Defines how many packets it takes for the sensor to positively identify an alarm condition on the network. There are two signature structure types:
  - Atomic signature—Requires only one packet to be inspected to identify an alarm condition.
  - Composite signature—Requires multiple packets to be inspected to identify an alarm condition.

  In Figure 105, the Signature Structure is Atomic.
- Implementation—The signatures examine the packet headers to identify an alarm condition. There are two implementation types:
  - Content-based signatures—Examine the payload and headers of a packet to identify an alarm condition.
  - Context-based signatures—Evaluate the packet headers to identify an alarm condition.

  In Figure 105, the Implementation is Content.
- Release Version—This number indicates in which release this signature originated. In Figure 105, it is release 2.2.1.5.
- Description—A concise explanation of the signature and what exploits it detects.
- Benign Trigger(s)—A concise explanation of any activity that may appear to be an exploit but are actually normal network activity.
- Data Field Information Tag—Provides a bit of the information used to create a signature, such as an example URL.
- Related Vulnerabilities—Each signature can have zero or more related vulnerabilities. Each vulnerability information page provides background on the vulnerability and a link to any available countermeasures.
- User Notes—The user-defined notes page is an empty template in which you can fill in security information customized to your network security environment.

ECT 4077 U 1

Figure 105 IP Fragment Incomplete Datagram NSDB Entry



Managing Data

For information on setting up, viewing, and managing events from up to three sensors, refer to the *Cisco Intrusion Detection System Event Viewer Configuration Note Version 3.1* found at the following website:

http://www.cisco.com/univercd/cc/td/doc/product/iaabu/csids/csids8/index.htm

Troubleshooting

Use the following sensor commands when troubleshooting issues with TAC:

- If you have difficulty connecting to the sensor through the IDS Device Manager, SSH or Telnet to the sensor and type the following command to check the version and status of the sensor (whether it is running):

  ```
  cidServer version
  ```

Note The server is started automatically at boot, so you do not need to start or stop it during normal use.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1178
Doc: 3701

- If the server is not running, start it by entering the following command:

```
cidServer start
```

- If you are troubleshooting an issue with TAC and you need to stop and start the server, enter the following commands:

```
cidServer stop
cidServer start
```

Glossary

The following list contains terms that are pertinent to Cisco IDS.

Numerals

3DES Triple Data Encryption Standard. A stronger version of DES, which is the default encryption method for SSH v.1.

A

AAA authentication, authorization, and accounting. A Cisco IOS Software and PIX Firewall command for controlling how users can log into a router or a PIX Firewall.

ACE access control entry. An entry in the ACL that describes what action should be taken for a specified address or protocol.

ACK Notification sent from one network device to another to acknowledge that some event occurred (for example, the receipt of a message).

ACL access control list. The means by which access to, and denial of, services is controlled. It is a list of the services available, each with a list of the hosts permitted to use the service.

active ACL The ACL created and maintained by device management (*managed*) and applied to the router block interfaces.

alarm An IDS message that is used internally to indicate a network exploit in progress or a potential security problem occurrence.

attack An assault on system security that derives from an intelligent threat, that is, an intelligent act that is a deliberate attempt (especially in the sense of a method or technique) to evade security services and violate the security policy of a system.

authentication Used to describe the hash key value, usually a 32-byte hexadecimal value.

4075

B

benign trigger A situation in which a signature is fired correctly, but the source of the traffic is nonmalicious.

blocking Refers to the ability of the sensor to use a network device to deny entry to a specific network host or an entire network. See blocking.

C

C & C command and control. Refers to the network interface on a sensor through which it is managed.

cipher key Used to describe the encryption key value. For Data Encryption Standard (DES), a valid encryption key is a 16-byte hexadecimal value.

CiscoFusion Cisco internetworking architecture that "fuses" together the scalability, stability, and security advantages of the latest routing technologies with the performance benefits of ATM and LAN switching, and the management benefits of VLANs. See Cisco IOS.

Cisco IOS Cisco Internetworking Operating System. Cisco Systems software that provides common functionality, scalability, and security for all products under the CiscoFusion architecture. Cisco IOS software allows centralized, integrated, and automated installation and management of internetworks, while ensuring support for a wide variety of protocols, media, services, and platforms. See CiscoFusion.

Cisco Secure Policy Manager Cisco Secure Policy Manager is a scalable, comprehensive security policy management system.

configuration management Configuration management refers to the ability of the IDS manager to remotely manage the configuration of sensors. This ability allows network security personnel to centrally manage all the sensors across an enterprise-wide collection.

control interface When device management (*managed*) opens a Telnet or SSH session with a network routing device, it uses one of the routing interfaces of the device as the remote IP address. This is the control interface.

countermeasure An action, device, procedure, or technique that reduces a threat, a vulnerability, or an attack by eliminating or preventing it, by minimizing the harm it can cause, or by discovering and reporting it so that corrective action can be taken.

D

daemon/service A daemon or service performs a specific function, such as writing log files, analyzing IP traffic, or processing events.

ROS Nº 03/2005 - CN
CPMI - CORREIOS
1179
Fls:
Doc: 3701

DES Data Encryption Standard. A strong encryption method where the strength lies in a 56-bit key rather than an algorithm.

device management Device management refers to the ability of the sensor to interact with network devices. For example, it can dynamically reconfigure the ACLs of a router to block an attacker. Device management is controlled by the *managed* service.

director The director is the UNIX-based IDS manager. A single director can manage and monitor a group of sensors, which enables security personnel to secure a network from a centralized console.

DNS Domain Name System. An Internet-wide host name to IP address mapping. DNS enables you to convert human-readable names into the IP addresses needed for network packets.

DoS Denial of Service. A denial of service attack is an attack whose goal is just to disrupt the operation of a specific system or network.

E

encryption Application of a specific algorithm to data so as to alter the appearance of the data making it incomprehensible to those who are not authorized to see the information.

engine A component of the sensor designed to support many signatures in a certain category. Each engine has parameters that can be used to create new signatures or tune existing signatures.

enterprise network Large and diverse network connecting most major points in a company or other organization. Differs from a WAN in that it is privately owned and maintained.

F

false negative A situation in which a signature is not fired when offending traffic is detected.

false positive A situation in which a signature is fired incorrectly.

filtering router An internetwork router that selectively prevents the passage of data packets according to a security policy.

firewall A security device that protects the perimeter of the network.

fragmentation IP fragmentation involves breaking a single IP packet into multiple segments that are all below the maximum transmission size for the network.

H

HTTP — Hypertext Transfer Protocol. The standard protocol used by websites to convey information to web users. By default, this protocol uses TCP port 80.

HTTPS — An extension to the standard HTTP protocol that provides confidentiality by encrypting the traffic from the website. By default this protocol uses TCP port 443.

I

ICMP — Internet Control Message Protocol. Network layer Internet protocol that reports errors and provides other information relevant to IP packet processing. Documented in RFC 792.

IETF — Internet Engineering Task Force. Task force consisting of over 80 working groups responsible for developing Internet standards. The IETF operates under the auspices of ISOC.

intrusion detection — A security service that monitors and analyzes system events for the purpose of finding, and providing real-time or near real-time warning of, attempts to access system resources in an unauthorized manner.

Intrusion Detection Planning Guide — Describes intrusion detection technology and provides basic design considerations and scenarios for deployment.

IDM — Intrusion Detection System Device Manager. A web-based device manager for sensors. The IDM provides basic configuration and management capability.

IDS MC — Management Center for IDS Sensors. Web-based IDS manager can manage configurations for up to 300 sensors.

IDV — Intrusion Detection System Device Viewer. The IDV provides basic monitoring and reporting capability to complement the web-based IDM.

IP address — 32-bit address assigned to hosts using TCP/IP. An IP address belongs to one of five classes (A, B, C, D, or E) and is written as 4 octets separated by periods (dotted decimal format). Each address consists of a network number, an optional subnetwork number, and a host number. The network and subnetwork numbers together are used for routing, and the host number is used to address an individual host within the network or subnetwork. A subnet mask is used to extract network and subnetwork information from the IP address.

IPSec — IP Security Protocol. A framework of open standards that provides data confidentiality, data integrity, and data authentication between participating peers. IPSec provides these security services at the IP layer. IPSec uses IKE to handle negotiation of protocols and algorithms based on local policy and to generate the encryption and authentication keys to be used by IPSec. IPSec can be used to protect one or more data flows between a pair of hosts, between a pair of security gateways, or between a security gateway and a host.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1180
Doc: 3701

IP spoofing IP spoofing attack occurs when an attacker outside your network pretends to be a trusted user either by using an IP address that is within the range of IP addresses for your network or by using an authorized external IP address that you trust and to which you want to provide access to specified resources on your network. Should an attacker get access to your IPSec security parameters, that attacker can masquerade as the remote user authorized to connect to the corporate network.

ISOC Internet Society. International nonprofit organization, founded in 1992, that coordinates the evolution and use of the Internet. In addition, ISOC delegates authority to other groups related to the Internet, such as the IAB. ISOC is headquartered in Reston, Virginia (United States).

L

logging Logging of security information is performed on two levels: logging of events (such as IDS commands, errors, and alarms), and logging of individual IP session information.

M

manager Used to describe the node managing the IDS sensor, for example one of the following: IDS Director, CSPM, IDM, or IDS MC.

managed Service responsible for managing and monitoring network devices (routers and packet filters

MTU Maximum Transmission Unit. Represents the maximum packet size that a network segment can handle. If a packet is larger than the MTU, the sending host breaks it into multiple frames and then transmits the multiple frames across the network for reassembly at the destination host.

N

network device A router or packet filter, especially one that works with a sensor to block or cut unauthorized connections.

nrConfigure The Java-based tool for centralized configuration management of remote sensors used by the IDS Director.

NSDB Network Security Database. A database of security information that explains the signatures used by your IDS along with the vulnerabilities on which these signatures are based.

P

packetd — Service that provides intrusion detection; *packetd* is used when the sensor itself is capturing packets directly from the network.

PIX Firewall — Private Internet Exchange Firewall. A Cisco network security device that can be programmed to block/enable addresses and ports between networks.

postoffice — The proprietary protocol that maintains communication across a network between IDS services.

R

regular expression — A mechanism by which you can define how to search for a specified sequence of characters in a data stream or file.

RPC — remote-procedure call. Technological foundation of client/server computing. RPCs are procedure calls that are built or specified by clients and are executed on servers, with the results returned over the network to the clients.

RSA — Acronym stands for Rivest, Shamir, and Adelman, the inventors of the technique. Public-key cryptographic system which may be used for encryption and authentication.

S

SA — Security association. An instance of security policy and keying material applied to a data flow.

Security Monitor — Monitoring Center for Security. Provides event collection, viewing, and reporting capability for network devices. Used with the IDS MC.

sensor — The sensor is the intrusion detection engine. It analyzes network traffic, searching for signs of unauthorized activity.

sensor fidelity — A sensor has good fidelity if it does not exhibit false positives or false negatives and exhibits true positives and true negatives and minimized benign triggers. Signature threshold tuning may be necessary to achieve fidelity.

shunning — Shunning refers to the ability of the sensor to use a network device to deny entry to a specific network host or an entire network. See blocking.

signature — A signature distills network information and compares it against a rule set that indicates typical intrusion activity.

signature inspector — The subsystem that inspects aggregate traffic for known signatures.

RQS Nº 05/2005 - CN
CPMI - CORREIOS
Fls: 1181
Doc: 3701

SPAN Switched Port Analyzer. Feature of the Catalyst 5000 switch that extends the monitoring abilities of existing network analyzers into a switched Ethernet environment. SPAN mirrors the traffic at one switched segment onto a predefined SPAN port. A network analyzer attached to the SPAN port can monitor traffic from any of the other Catalyst switched ports.

SPI Security Parameter Index. A 32-bit entity used to uniquely identify an SA at the receiver. Value ranges are 0x100 - 0xffff ffff (numeric).

SSH Secure Shell. A utility that provides a remote secure C & C interface so the sensor can be configured without exposing plain text user names or passwords to the network connecting the remote user to the sensor.

SSL Secure Socket Layer. Encryption technology for the Web used to provide secure transactions, such as the transmission of credit card numbers for e-commerce.

subsignature A more granular representation of a general signature. They typically further define a broad scope signature.

sysconfig-sensor The program used to initialize the sensor and set up communications between it and the IDS manager.

SYN flood Denial of service attack that sends a host more TCP SYN packets (request to synchronize sequence numbers, used when opening a connection) than the protocol implementation can handle

T

TACACS Terminal Access Controller Access Control System. Authentication protocol, developed by the DDN community, that provides remote access authentication and related services, such as event logging. User passwords are administered in a central database rather than in individual routers, providing an easily scalable network security solution.

TACACS+ Terminal Access Controller Access Control System Plus. Proprietary Cisco enhancement to Terminal Access Controller Access Control System (TACACS). Provides additional support for authentication, authorization, and accounting.

TCP Transmission Control Protocol. Connection-oriented transport layer protocol that provides reliable full-duplex data transmission. TCP is part of the TCP/IP protocol stack.

Telnet Standard terminal emulation protocol in the TCP/IP protocol stack. Telnet is used for remote terminal connection, enabling users to log in to remote systems and use resources as if they were connected to a local system. Telnet is defined in RFC 854.

threshold A value, either upper- or lower-bound that defines the maximum/minimum allowable condition before an alarm is sent.

TLS Transport Layer Security. A future IETF protocol to replace SSL.

E
24.069
1
v

traffic analysis	Inference of information from observable characteristics of data flow(s), even when the data is encrypted or otherwise not directly available. Such characteristics include the identities and locations of the source(s) and destination(s), and the presence, amount, frequency, and duration of occurrence.
true negative	A situation in which a signature is not fired when nonoffending traffic is detected.
true positive	A situation in which a signature is fired properly when the offending traffic is detected.

U

UDP	User Datagram Protocol. Connectionless transport layer protocol in the TCP/IP protocol stack. UDP is a simple protocol that exchanges datagrams without acknowledgments or guaranteed delivery, requiring that error processing and retransmission be handled by other protocols. UDP is defined in RFC 768.

V

VACL	VLAN ACL. An ACL that filters all packets (both within a VLAN and between VLANs) that pass through a switch. Also known as a Security ACL.
VLAN	virtual LAN. A logical division of a LAN into different broadcast domains.
vulnerability	One or more attributes of a computer or a network that permit a subject to initiate patterns of misuse on that computer or network.

Related Documentation

This document should be used in conjunction with the following publications:

- *Cisco Intrusion Detection System Sensor Installation and Safety Note*
- *Cisco Intrusion Detection System Sensor Accessories Contents and Installation Instructions*
- *Cisco Intrusion Detection System Getting Started Version 3.1*
- *Cisco Intrusion Detection System Sensor Configuration Note Version 3.1*
- *Cisco Intrusion Detection System Signature Engines Version 3.1*
- *Release Notes for Cisco Intrusion Detection System Sensor Version 3.1*
- *Cisco Intrusion Detection System Device Manager Version 3.1*
- *Cisco Intrusion Detection System Event Viewer Version 3.1*

RQS Nº 03/2005 - CN -
CPMI - CORREIOS
1182
Fls:
3701

For additional information on the Cisco Intrusion Detection System, refer to the following documentation:

- *Cisco Intrusion Detection System Director for UNIX Configuration and Operations Guide Version 2.2.3*
- *Release Notes for Cisco Intrusion Detection System Director for UNIX Version 2.2.3*
- *Cisco Secure Policy Manager Solution Guide Series: Intrusion Detection System, Version 2.3.1i*
- *Cisco Secure Policy Manager Installation Guide, Version 2.3.1i*
- *Release Notes for Cisco Secure Policy Manager Version 2.3i*
- *Catalyst 6000 Intrusion Detection System Module Installation and Configuration Note Version 3.0*
- *Release Notes for Catalyst 6000 Intrusion Detection System Module Software Release 3.5(1)S4*
- *Intrusion Detection Planning Guide*

Obtaining Documentation

The following sections explain how to obtain documentation from Cisco Systems.

World Wide Web

You can access the most current Cisco documentation on the World Wide Web at the following URL:

http://www.cisco.com

Translated documentation is available at the following URL:

http://www.cisco.com/public/countries_languages.shtml

Documentation CD-ROM

Cisco documentation and additional literature are available in a Cisco Documentation CD-ROM package, which is shipped with your product. The Documentation CD-ROM is updated monthly and may be more current than printed documentation. The CD-ROM package is available as a single unit or through an annual subscription.

Ordering Documentation

Cisco documentation is available in the following ways:

- Registered Cisco Direct Customers can order Cisco product documentation from the Networking Products MarketPlace:

  http://www.cisco.com/cgi-bin/order/order_root.pl

- Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:

  http://www.cisco.com/go/subscription

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco corporate headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

If you are reading Cisco product documentation on Cisco.com, you can submit technical comments electronically. Click **Leave Feedback** at the bottom of the Cisco Documentation home page. After you complete the form, print it out and fax it to Cisco at 408 527-0730.

You can e-mail your comments to bug-doc@cisco.com.

To submit your comments by mail, use the response card behind the front cover of your document, or write to the following address:

Cisco Systems
Attn: Document Resource Connection
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Obtaining Technical Assistance

Cisco provides Cisco.com as a starting point for all technical assistance. Customers and partners can obtain documentation, troubleshooting tips, and sample configurations from online tools by using the Cisco Technical Assistance Center (TAC) Web Site. Cisco.com registered users have complete access to the technical support resources on the Cisco TAC Web Site.

Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world.

Cisco.com is a highly integrated Internet application and a powerful, easy-to-use tool that provides a broad range of features and services to help you to

- Streamline business processes and improve productivity
- Resolve technical issues with online support

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1183
Doc: 3701

- Download and test software packages
- Order Cisco learning materials and merchandise
- Register for online skill assessment, training, and certification programs

You can self-register on Cisco.com to obtain customized information and service. To access Cisco.com, go to the following URL:

http://www.cisco.com

Technical Assistance Center

The Cisco TAC is available to all customers who need technical assistance with a Cisco product, technology, or solution. Two types of support are available through the Cisco TAC: the Cisco TAC Web Site and the Cisco TAC Escalation Center.

Inquiries to Cisco TAC are categorized according to the urgency of the issue:

- Priority level 4 (P4)—You need information or assistance concerning Cisco product capabilities, product installation, or basic product configuration.
- Priority level 3 (P3)—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- Priority level 2 (P2)—Your production network is severely degraded, affecting significant aspects of business operations. No workaround is available.
- Priority level 1 (P1)—Your production network is down, and a critical impact to business operations will occur if service is not restored quickly. No workaround is available.

Which Cisco TAC resource you choose is based on the priority of the problem and the conditions of service contracts, when applicable.

Cisco TAC Web Site

The Cisco TAC Web Site allows you to resolve P3 and P4 issues yourself, saving both cost and time. The site provides around-the-clock access to online tools, knowledge bases, and software. To access the Cisco TAC Web Site, go to the following URL:

http://www.cisco.com/tac

All customers, partners, and resellers who have a valid Cisco services contract have complete access to the technical support resources on the Cisco TAC Web Site. The Cisco TAC Web Site requires a Cisco.com login ID and password. If you have a valid service contract but do not have a login ID or password, go to the following URL to register:

http://www.cisco.com/register/

If you cannot resolve your technical issues by using the Cisco TAC Web Site, and you are a Cisco.com registered user, you can open a case online by using the TAC Case Open tool at the following URL:

http://www.cisco.com/tac/caseopen

If you have Internet access, it is recommended that you open P3 and P4 cases through the Cisco TAC Web Site.

4.065
2

Cisco TAC Escalation Center

The Cisco TAC Escalation Center addresses issues that are classified as priority level 1 or priority level 2; these classifications are assigned when severe network degradation significantly impacts business operations. When you contact the TAC Escalation Center with a P1 or P2 problem, a Cisco TAC engineer will automatically open a case.

To obtain a directory of toll-free Cisco TAC telephone numbers for your country, go to the following URL:

http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml

Before calling, please check with your network operations center to determine the level of Cisco support services to which your company is entitled; for example, SMARTnet, SMARTnet Onsite, or Network Supported Accounts (NSA). In addition, please have available your service agreement number and your product serial number.

This document is to be used in conjunction with the documents listed in the "Related Documentation" section.

CCIP, the Cisco *Powered* Network mark, the Cisco Systems Verified logo, Cisco Unity, Follow Me Browsing, FormShare, Internet Quotient, iQ Breakthrough, iQ Expertise, iQ FastTrack, the iQ Logo, iQ Net Readiness Scorecard, Networking Academy, ScriptShare, SMARTnet, TransPath, and Voice LAN are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, Discover All That's Possible, The Fastest Way to Increase Your Internet Quotient, and iQuick Study are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE

Copyright © 2002, Cisco Systems, Inc.
All rights reserved.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1184
Fls:
3701
Doc:

Apêndice CM

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1185
Doc: 3701

E Q & A
4.063

Cisco Secure Intrusion Detection System

Q. What is the Cisco Secure Intrusion Detection System (IDS)?

A. The Cisco Secure IDS is an enterprise-class, network-based intrusion-detection system. Designed to address the increased requirements for security visibility, denial-of-service (DoS) protection, antihacking detection, and e-commerce business defenses, the Cisco Secure IDS family leads the market in innovative security monitoring solutions. Sensor devices detect unauthorized activity traversing the network, such as attacks by hackers, by analyzing traffic in real time, enabling users to quickly respond to security breaches. When unauthorized activity is detected, Sensors can send alarms to a management console with details of the activity and can control other systems, such as routers, to terminate the unauthorized session(s).

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. The implementation of these systems is in the form of small clients or applications. Host-based systems require the use of the resources of a host server—disk space, RAM, and CPU time, a setup that impacts system performance. Intrusions are detected primarily by analyzing operating-system audit trails, application audit trails, and other system activity. Host-based IDSs are ideal if a limited number of critical servers must be protected, but they do not scale well if enterprise-wide solutions are needed.

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 Secure Intrusion Detection System, a network-based IDS, provides network administrators with enhanced security technology and capabilities to secure their networks.

Public
Copyright © 2000 Cisco Systems, Inc. All Rights Reserved.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1186
3701
Doc:

E C T
4.062
L
S L - D.C.

Q. How does the Cisco Secure Intrusion Detection System fit into the Cisco end-to-end security strategy known as the Cisco SAFE blueprint for secure e-business?

SAFE is a comprehensive security blueprint that tells organizations how to safely engage in e-Business today.

Developed for real-world network deployment, SAFE helps customers compete in the Internet Economy by integrating scalable, high performance security services throughout the e-Business infrastructure. It takes a simplified, modular approach to security in which design, implementation and management processes are all detailed for the customer. The customer 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. This modular approach gives customers the flexibility to deploy SAFE in stages, allowing organizations to leverage their existing security infrastructure while staying within budget on new e-Business initiatives.

SAFE will help companies prepare for the convergence of data, voice and video over Internet Protocol (IP) based networks. Built on Cisco AVVID—the Architecture for Voice, Video and Integrated Data—SAFE provides companies with a secure, cost-effective migration path to converged networks.

A key advantage of SAFE is that, in an increasingly connected world, where executives are questioning whether securing the perimeter is enough, SAFE delivers answers for fully protecting every access point to the network. Indeed, SAFE is enhanced by a rich ecosystem of programs, products, partners and services—all addressing the key requirements for safeguarding a network: secure connectivity, perimeter security, security monitoring, identity and security management.

The Cisco Secure Intrusion Detection System is a dynamic security component of the SAFE security blueprint which includes ...walls, virtual private networks (VPNs), and authentication products. When used in conjunction with firewalls, encryption, authentication, and active audit, the system allows customers to build and operate secure electronic business environments.

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. What components are required to deploy Cisco Secure IDS?

A. A Cisco Secure IDS installation consists of the following:

...e installation has at least one management console, which provides a visual alarm display and a remote system configuration utility. Multiple management consoles can be deployed for larger, distributed environments.

- One or more sensors is deployed strategically on your production network(s). The sensors analyze and detect unauthorized activity traversing the network; send alarms back to a central management console; and they can be configured to respond to these events by terminating the offending session(s). Sensors can be configured to send alarms to multiple management consoles simultaneously, allowing deployments to scale in large enterprise environments.

Copyright © 2000 Cisco Systems, Inc. All Rights Reserved.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1187
Fls: 3701
Doc:

Q. What management console options are available for the Cisco Secure IDS?

A. A management console, which provides a visual alarm graphical user interface (GUI) display and a remote system configuration utility, is required for the Cisco Secure IDS. Current offerings include:

- Cisco Secure IDS Director—HP OpenView Network Node Manager "plug-in" that runs on UNIX (Solaris and HP-UX)
- Cisco Secure Policy Manager (v2.2+)—Windows NT-based package

Alarm viewing, analysis and reporting packages are also available from Cisco Security Associates partners (see: http://www.cisco.com/warp/public/778/security/sap/management.html)

Q. What sensor options are available for the Cisco Secure IDS?

A. The current Cisco Secure IDS sensing portfolio includes:

- Catalyst® 6000 IDS Module—Full-featured IDS module that occupies one slot in a Catalyst 6x000 chassis
- Network Sensor appliances—IDS-4230 and IDS-4210 "plug-and-play" appliances

Q. How does the 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, "si ures"). 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. Where should sensors be installed?

A. Sensors may be placed on almost any network segment of the enterprise-wide network where security visibility is required; for example:

- Internal network segments where critical resources are located
- In front of a firewall
- Behind a firewall
- Behind a dialup modem server
- At extranet connections
- On the DMZ

When deploying sensors, you must install them so that they can "see" the network traffic that you want to monitor. This is typically done with shared-media hubs or SPAN ports on switches.

Q. How do you deploy sensors in a switched environment?

A. h most IDS products on the market today, sensors must be placed on the switch SPAN port to monitor network traffic. This is the case for the Cisco Secure IDS appliance sensors as well. Although the SPAN port can provide access to network traffic, it does have certain limitations (for example, limited number of SPAN sessions, trunked traffic). 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 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).

Copyright © 2000 Cisco Systems, Inc. All Rights Reserved.

RQS Nº 03/2005 - CPMI - CORREIOS
1188
Fls:
3701
Doc:

4060

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 types of attacks does the Cisco Secure IDS detect?

A. The Cisco Secure Intrusion Detection System has the most extensive and comprehensive signature list designed to detect attacks in all of the following categories:

- Exploits—Activity indicative of someone attempting to gain access or compromise systems on your network, such as Back Orifice, failed login attempts, and TCP hijacking
- DoS—Activity indicative of someone attempting to consume bandwidth or computing resources to disrupt normal operations, such as Trinoo, TFN, and SYN floods
- Reconnaissance—Activity indicative of someone probing or mapping your network to identify "targets of opportunity," such as g sweeps and port sweeps; usually a precursor to an actual exploit attempt
- Misuse—Activity indicative of someone attempting to violate corporate policy; this can be detected by configuring the sensor to look for custom text strings in the network traffic; for example, XYZ Corporation could easily configure the Cisco Secure IDS to send an alarm on and eliminate any connection that transmits the phrase "XYZ Confidential" in e-mail or File Transfer Protocol (FTP).

Q. Which protocols can the Cisco Secure IDS monitor?

A. The Cisco Secure Intrusion Detection System can monitor all of the major TCP/IP protocols, including IP, Internet Control Message Protocol (ICMP), TCP, and User Datagram Protocol (UDP). It can also statefully decode application-layer protocols such as FTP, Simple Mail Transfer Protocol (SMTP), HTTP, Domain Name System (DNS), remote procedure call (RPC), NetBIOS, NNTP and Telnet.

Q. Do the Cisco Secure IDS sensors reassemble fragmented packets to detect fragmented attacks?

A. Yes, the IDS-4230, IDS-4210 and the Catalyst 6000 IDS Module all reassemble fragmented packets to detect attacks that use fragmentation to evade the IDS.

Q. Can I create my own signatures?

A. Cisco Secure IDS users can easily create custom string-based signatures for immediate defense from certain attacks, for example, detecting e-mail attachments with the .vbs file extension to identify the I LOVE YOU worm. This same capability can be used to h for data unique to the customer environment. For example, XYZ Corporation could easily configure the Cisco Secure IDS to detect and eliminate any connection that transmits the phrase "XYZ Confidential" in e-mail or FTP.

Q. How difficult is it to install a Cisco Secure IDS sensor?

A. Appliance sensors were designed for technician-level installation, requiring the sensors to be simply plugged into the network, turned on, and configured with several simple initialization parameters. These parameters include standard network items such as IP address, host name, network masks, management console IP address, and so forth. Installation of the Catalyst 6000 IDS Module requires sliding the module into an open chassis slot, configuring the module with the parameters similar to configuration of the appliance, and configuring the switch to recognize the card and send traffic to it. After the sensors are initialized and running, configurations can be modified and pushed to them from Cisco Secure Policy Manager (CSPM) or the Cisco Secure IDS Director.

RQS Nº 03/2005 - CN -
CPMI - CORREIOS
1189
Fls:
3701
Doc:

Copyright © 2000 Cisco Systems, Inc. All Rights Reserved.

Q. How easy is it to replace a sensor that fails?

A. If a sensor (either an appliance or the Catalyst 6000 IDS Module) fails, you simply remove the failed unit and replace it with a new one. Initializing the new unit requires only that you configure it with the same initialization parameters that were configured on the failed unit, such as the IP address, host name, network masks, management console IP address, and so forth. The configuration of the failed unit, which is stored on the CSPM or Cisco Secure IDS Director platform, can be quickly pushed to the new sensor and the sensor is back on line.

Q. How many false positives will the Cisco Secure IDS generate?

A. False positives occur when an IDS mistakenly reports certain benign activity as malicious, requiring human intervention to diagnose the event. Obviously, false positives are undesirable because they consume valuable human resources. Although all IDS products on the market today are subject to false positives, special care is taken when the Cisco Secure IDS signatures are designed in order to minimize the occurrence of false positives, and they are tested extensively to validate the design. The sensors also provides very flexible and easy-to-use "tuning" functionality to allow users to instruct the sensors to not alarm based on certain parameters, such as by signature type and source or destination IP address. A specific example is where an authorized network management system performing node discovery triggers the ping sweep signature. Although ping sweeps can be indicative of malicious reconnaissance activity, this alarm is clearly a false positive because the source is an authorized network management system. To prevent this false positive from reoccurring, the user can configure the sensor to not alarm on ping sweeps from the network management system IP address. With this configuration, however, any other attacks that originate from that device will be disc[illegible]red. Sensor tuning to reduce false positives will probably be required during installation of any new sensor.

Q. Can the sensor detect attacks if the traffic is encrypted, for example IPSecurity (IPSec) or Secure Sockets Layer (SSL)?

A. The Cisco Secure 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 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 Secure 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. How are the Cisco Secure IDS signatures updated?

A. Cisco posts signature updates on Cisco Connection Online (CCO) approximately every 60 days (additional releases may be required in extraordinary situations). Customers with maintenance agreements can download and install the signature updates. Installing the update on the sensor will not overwrite any changes the user may have made in customizing the configuration.

Q. How can the Cisco Secure IDS Sensors respond to stop attacks?

A. In addition to sending alarms, appliance sensors can be configured to automatically respond to attacks by applying access control lists (ACLs) on specified Cisco routers to block all traffic from the attack source or to send out TCP reset packets to break any established connections from the attack source. Response actions are not currently supported in the Catalyst 6000 IDS Module, but will be in the future.

Q. How do the Cisco Secure IDS Sensors and management consoles communicate with each other?

A. Communication between the Cisco Secure IDS Sensors and management consoles is provided by a proprietary, reliable UDP transport protocol that guarantees transmission to intended recipients and maintains connection status with all of the IDS components. 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.

Public
Copyright © 2000 Cisco Systems, Inc. All Rights Reserved.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1190
Fls:
3701
Doc:

E C
4.058
Brent
C P I

Q. How much additional network traffic does the Cisco Secure IDS generate?

A. Because each alarm and acknowledgement is contained in a single UDP packet, there is negligible impact on network traffic.

Q. Are Cisco Secure IDS communications encrypted?

A. IPSec functionality is included on the appliance Sensors to allow customers to encrypt traffic to management consoles with IPSec capabilities, CSPM for example. IPSec is also planned for the Cisco Secure IDS Module in the future.

Q. If I lose connectivity to a remote sensor, can I tell from the management console?

A. Both CSPM and the Cisco Secure IDS Director 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 CSPM and Cisco Secure IDS Director, 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 CSPM or Cisco Secure IDS Director platform, can be quickly pushed to the new sensor.

Q. Does the Cisco Secure IDS Director require HP OpenView Network Node Manager?

A. Cisco Secure IDS Director does require HP OpenView Network Node Manager, and it does not come with the Director. It must be purchased separately by the customer.

Q. How difficult is it to install the Cisco Secure IDS Director?

A. Installing the Director software on a Solaris or HP-UX platform with HP OpenView Network Node Manager preinstalled is very easy. The install is completely scripted and the user is prompted for a minimal amount of information during the install process. When installed and running, the Director will prompt the user to begin establishing communications with the sensors. As each sensor is contacted, the default configuration parameters are pulled back to the Director and the user is prompted to customize the security policy for that sensor. When the user is finished setting up the new policy parameters, they are stored on the Director and pushed back out to the sensor, where they are immediately enforced.

Q. How many sensors can one Cisco Secure IDS Director manage?

A. Although the technical limit is very large (greater than 1000), Cisco typically recommends a ratio of 20 to 25 ensors per Director 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 directors can be installed to scale the number of sensors.

Q. Can I have multiple Cisco Secure IDS Directors?

A. The Cisco Secure IDS architecture supports the deployment of multiple director platforms. Sensors can send alarms to multiple directors simultaneously, and directors can forward alarms to other directors, allowing customers to build large, hierarchical management infrastructures.

Q. Besides the GUI, how can the Cisco Secure IDS Director notify me when it receives an alarm?

A. The Cisco Secure IDS Director provides e-mail notification and custom script execution functionality in addition to an iconic alarm display. Taking advantage of HP OpenView functionality, the Director can also send out Simple Network Management Protocol (SNMP) traps with the alarm details.

Q. What skills are required to operate the Cisco Secure IDS?

A. Designing the IDS architecture and analyzing the alarms requires personnel with both security and networking knowledge. This is true for all IDS products on the market today.

Q. Does anyone offer a 24x7 managed IDS service using the Cisco Secure IDS?

A. Yes, numerous managed service providers offer a managed IDS service using the Cisco Secure IDS. These managed service providers include Exodus, AT&T, Counterpane, IBM Emergency Response Services, and NetSolve.

ROS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1191
Doc:
3701

Copyright © 2000 Cisco Systems, Inc. All Rights Reserved.

Q. Where can I get more detailed information on CSPM?

A. Information on CSPM can be found at http://www.cisco.com/go/policymanager.

Q. What type of Cisco service and support is provided for the Cisco Secure IDS?

A. The IDS-4230, IDS-4210, and Catalyst 6000 IDS Module sensors are covered by all six levels of SMARTnet™ maintenance. This includes hardware support as well as sensor software upgrades and access to the latest signatures posted on CCO. The Director software is covered by Software Application Support (SAS) and Software Application Support Plus Upgrades (SAU).

Q. Does Cisco offer a host-based intrusion-detection product?

A. No, Cisco has chosen to partner with a select set of vendors who offer a host-based IDS product. These Technology Partners have been signed up through the Cisco Security Associates program; they include the "entercept" product offered by ClickNet Software and the Vigilent product offered by PentaSafe Security Technologies.

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.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 Australia, Pty., Ltd
Level 17, 99 Walker Street
North Sydney
NSW 2059 Australia
www.cisco.com
Tel: +61 2 8448 7100
Fax: +61 2 9957 4350

Cisco Systems has more than 190 offices in the following countries. Addresses, phone numbers, and fax numbers are listed on the Cisco.com Web site at www.cisco.com/go/offices.

Argentina • Australia • Austria • Belgium • Brazil • Canada • Chile • China • Colombia • Costa Rica • Croatia • Czech Republic • Denmark • Dubai, UAE Finland • France • Germany • Greece • Hong Kong • 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 • Singapore Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela

Copyright © 2000, Cisco Systems, Inc. All rights reserved. SMARTnet is a trademark; and Catalyst, Cisco, Cisco IOS, Cisco Systems, and the Cisco Systems logo are registered trademarks of Cisco Systems, Inc. or its affiliates in the U.S. and certain other countries. All other trademarks mentioned in this document are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0007R)

09/00 LW

ROS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1192
Doc: 3701

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1193
Doc: 3701

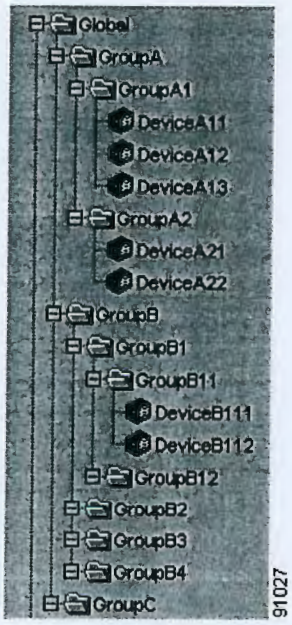
Adding Sensors and Sensor Groups

IDS MC uses a hierarchy of groups and sensors. A group can contain sensors, other groups, or a combination of sensors and groups. When you start IDS MC, you always have at least one active, defined group—the Global group. The IDS MC hierarchy can contain many *levels* of groups and sensors, just as a folder in Windows 2000 can contain many levels of folders and files. Figure 4-1 illustrates an example of the IDS MC hierarchy.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
4-1
Fls: 1194
Doc: 3701

ECT 055 CPL - AC

Figure 4-1 IDS MC Hierarchy Consisting of the Global Group, Groups, and Sensors



Notice the Global group in Figure 4-1.

The IDS MC hierarchy of groups and sensors enables you to configure more than one sensor at a time by configuring an entire group of sensors. Configuring more than one sensor at a time in this way is possible because a sensor can acquire settings from its parent group. A sensor *must*, in fact, acquire settings from its parent group if a parent defines those settings as mandatory. A child cannot override the values for such settings.

This chapter explains how to add groups and sensors to your IDS MC hierarchy and to perform other tasks.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
78-15615-01
1195
Fls:
Doc: 3701

Task List for Adding Sensors and Sensor Groups

From the Devices tab, you can add sensors that you want to manage with IDS MC. You can add and delete sensors, and you can add and delete sensor groups. However, you cannot delete the Global group. If you have established settings elsewhere, you can apply them to sensors and groups that you set up from the Devices tab.

For step-by-step procedures on performing a specific task, refer to the corresponding section.

- Adding Sensors to a Sensor Group, page 4-3
- Using SSH in IDS MC and Security Monitor, page 4-8
- Handling Rejected SSH Fingerprints, page 4-11
- Deleting Sensors from a Sensor Group, page 4-13
- Creating Sensor Subgroups, page 4-14
- Deleting Sensor Groups, page 4-16

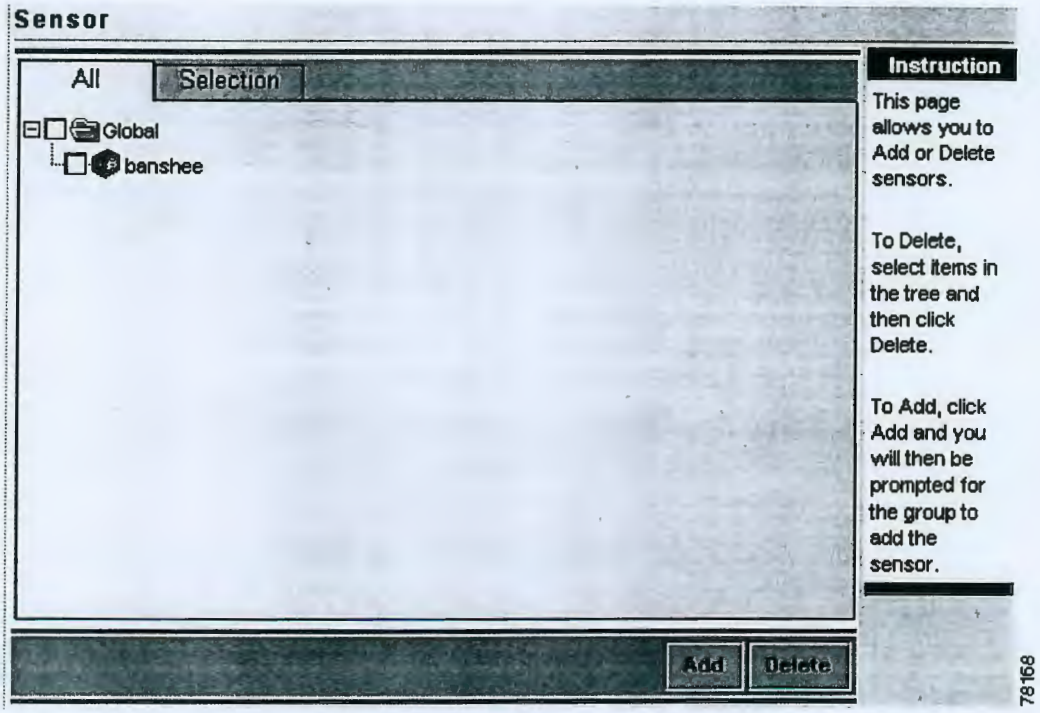
Adding Sensors to a Sensor Group

You can add a sensor to any sensor group, including the Global group.

To add a sensor to a sensor group, follow these steps:

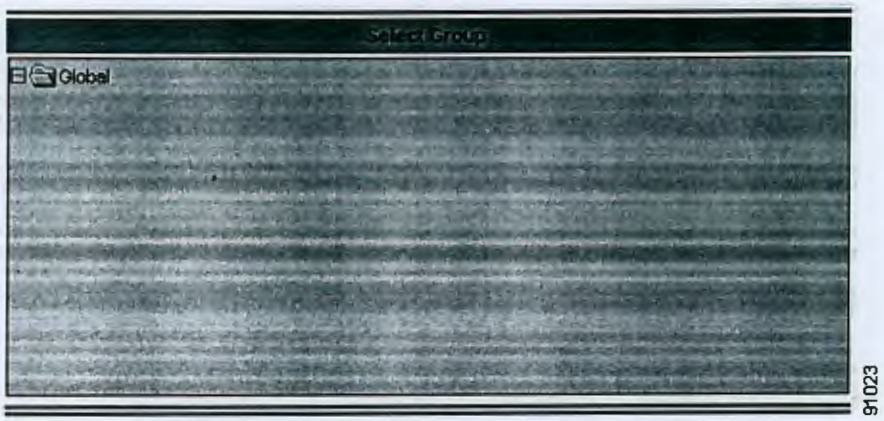
Step 1 Select **Devices > Sensor**.

The Sensor page appears.



Step 2 Click **Add**.

The Select Group page appears.

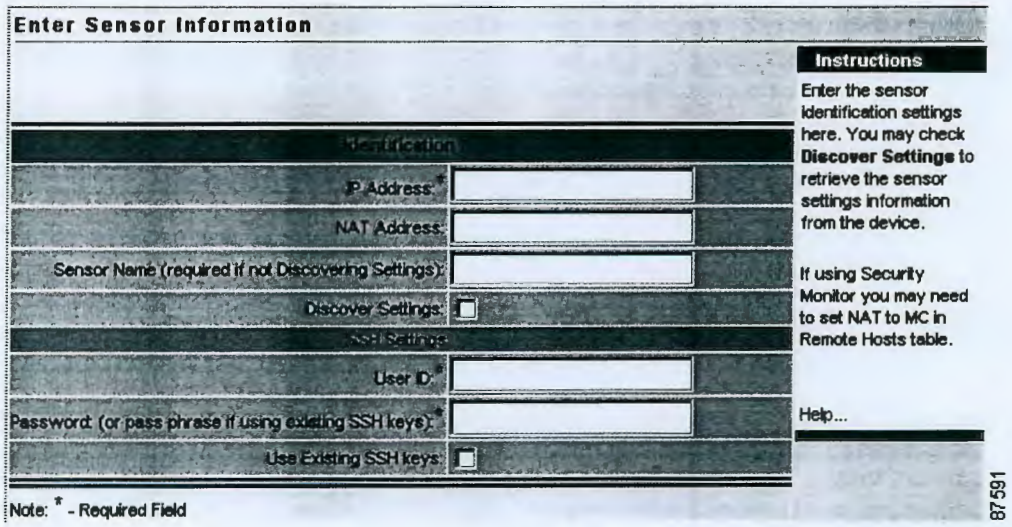


Step 3 Select the group you want to add a sensor to.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
78-15615-01
1197
Fls
Doc
3701

Step 4 Click **Next.**

The Enter Sensor Information page appears.



Step 5 Provide the information required by the Enter Sensor Information page:

a. Enter the IP address of the sensor.

b. Enter the NAT address of the sensor, if there is one.

c. Enter the sensor name.

d. To retrieve sensor settings from the sensor, select the **Discover Settings** check box.

Note If you choose to discover settings, you may have to wait from 30 seconds to several minutes, depending upon the size and complexity of your network and its traffic.

e. Enter the user ID and password for Secure Shell (SSH) communications between your host and the sensor:

- When you are using a sensor appliance, the user ID is **netrangr**, and the password is one that you assign.
- When you are using an IDS module, the user ID is **ciscoids**, and the password is one that you assign.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
4-5
Fls: 1198
Doc: 3701

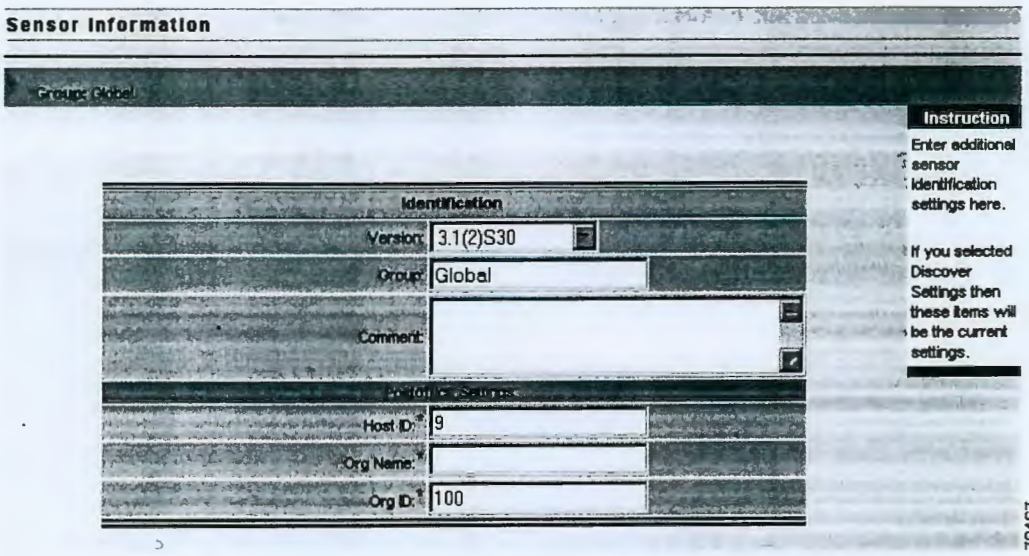
f. If you want to use existing SSH keys, select the check box associated with that option. However, you cannot use SSH keys if you intend to use this sensor as a master blocking sensor.

For more information, see Learn More About the Secure Shell Protocol, page 4-8. Also, see Using SSH in IDS MC and Security Monitor, page 4-8.

Note SSH supports two forms of authentication: password and public key. If you have set up a public key between IDS MC and the sensor, you can use that key by selecting the Use Existing SSH keys check box. If you have not set up the key, or if you do not want to use it, leave the Use Existing SSH keys deselected, and IDS MC will use SSH password authentication.

g. Click **Next**.

The Sensor Information page appears as follows in IDS MC 1.0 *and* in IDS MC 1.1 if the last sensor you added used sensor software version 3.x; a simplified version of this page appears in IDS MC 1.1 if the last sensor you added used sensor software version 4.x.



78-15615-01
ROS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1199
Doc: 3791

E C T
4.050
Jane
PL - AC

Step 6 If you are using IDS MC 1.0 *or* if you are using IDS MC 1.1 and adding a 3.x sensor, provide the following information in the Sensor Information page:

a. Select the version number that you are using from the Version list box. If you have reached this point, the version must be 3.x.

b. Enter a comment (optional).

c. Enter the Host ID (typically the last octet of the IP address of the sensor).

d. Enter the Org Name.

Note Use lowercase letters only in the Org Name field; do not use numbers, symbols, spaces, or capital letters. The Host ID and Org Name are case sensitive with respect to how postoffice processes audit events on the local host. Host names and Org Name values are not passed between different postoffice clients; only the Host ID and Org ID values are passed.

e. Enter the Org ID. The default value is 100.

Note Within a postoffice domain, no sensor or sensor group can have the same Org ID/Host ID pair as another sensor or sensor group.

Step 7 If you are using IDS MC 1.1 *and* you are adding a sensor operating with sensor software 4.x, provide the following information in the Sensor Information page:

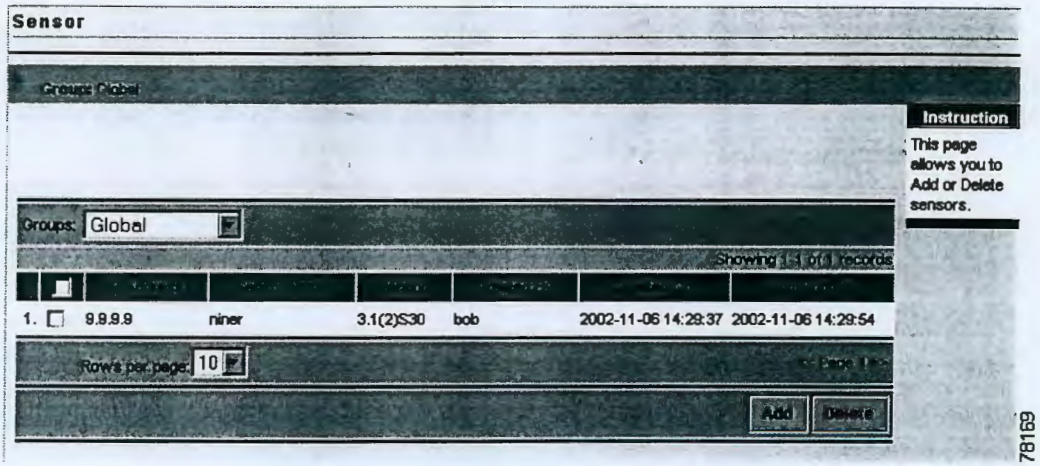
a. Select the version number that you are using from the Version list box. The version must be 4.x because you are using IDS MC 1.1.

b. Enter a comment (optional).

Step 8 Click **Finish**.

The Sensor page appears, updated with a record of the sensor you just added.

RQS Nº 03/2005 - CR
CPMI - CORREIOS
Fls: 1200
Doc: 3701



Learn More About the Secure Shell Protocol

Secure Shell (SSH) is a protocol for secure remote login and other secure network services over an insecure network. For more information about SSH, see *Designing Network Security* by Merike Kaeo (Indianapolis: Cisco Press, 1999).

Note IDS MC and Security Monitor make SSH available because of the importance of being able to transmit login information (including passwords) in an encrypted form.

The Secure Shell Working Group (SECSH) of the Internet Engineering Task Force (IETF) has the goal of updating and standardizing SSH. More information is available at http://www.ietf.org/html.charters/secsh-charter.html.

More information about using public keys for SSH authentication is available at http://www.chiark.greenend.org.uk/~sgtatham/putty/docs.html.

Using SSH in IDS MC and Security Monitor

IDS MC and Security Monitor support SSH for secure remote login to a sensor. Neither IDS MC nor Security Monitor manages SSH keys, however. The sensor software provides the SSH server, and IDS MC and Security Monitor provide

RQS Nº 03/2005 - CN
CPMI - CORREIOS
78-15615-01
Fls: 1201
Doc: 3701

support for an SSH Windows client—PuTTY. Documentation for PuTTY is available at http://www.chiark.greenend.org.uk/~sgtatham/putty/docs.html. More information about using public keys for SSH authentication is available at http://www.chiark.greenend.org.uk/~sgtatham/putty/docs.html.

Version 1.0 of IDS MC and Security Monitor uses PuTTY 0.51. Version 1.1 of IDS MC and Security Monitor uses PuTTY 0.53b.

Directions for using SSH keys with PuTTY are available at http://www.chiark.greenend.org.uk/~sgtatham/putty/docs.html.

PuTTY's Pageant utility is an SSH authentication agent. We recommend using Pageant to manage your keys in IDS MC. More information on Pageant is available at http://www.chiark.greenend.org.uk/~sgtatham/putty/docs.html.

Sensor appliances running IDS software versions 3.x and later, and IDSMs running IDS software 3.1(1) and later, have a `/usr/nr/.ssh` directory. You must create the authorized_keys file (if it does not exist) and then place that authorized_keys file in the `/usr/nr/.ssh` directory. Finally, you must place your public key in the authorized_keys file.

To use SSH keys in IDS MC or Security Monitor, follow these steps:

Step 1 Use PuttyGen to generate your keys. Instructions are available at http://www.chiark.greenend.org.uk/~sgtatham/putty/docs.html.

Step 2 Copy the public key to the sensor's `~.ssh/authorized_keys` file.

Step 3 Save the private key. We recommend the name `sensorname.key` for the private key and use it in this example.

Caution Guard your private key carefully because of its importance to the security of your network, and back it up to a secure location.

Step 4 Create a session for the sensor and perform the following steps:

a. At a command line prompt, enter **putty**.

b. Enter the hostname when prompted.

c. Click **Protocol SSH**.

d. Select **System > Saved Sessions**.

e. Select **sensorname.key** (the name of the saved session in this example) from the list box.

RQS Nº 03/2005 - C
C MI - CORREIOS
4-9
Fls: 1202
Doc: 3701

E C
4047
Doc

f. Click **Load**.

   Your saved settings appear in the configuration panel.

g. Click **Connection**.

h. Enter the auto-login username: **netrangr**.

i. Click **session**.

j. Click **SSH**.

k. Enter the private key file for authentication: **sensorname.key**.

l. Enter **save**.

m. Enter **cancel**.

n. Enter **putty@***host name*.

You will be prompted for the passphrase that you generated in Step 1.

Learn More About SSH Fingerprints

SSH fingerprints are described in the following material, which is quoted verbatim from the *PuTTY User Manual* (http://www.chiark.greenend.org.uk/~sgtatham/putty/docs.html). PuTTY is copyright 1997-2001 Simon Tatham.

"If you are using SSH to connect to a server for the first time, you will probably see a message [similar to the following]:

```
"The server's host key is not cached in the registry. You have no
guarantee that the server is the computer you think it is.

"The server's key fingerprint is: ssh-rsa 1024
7b:e5:6f:a7:f4:f9:81:62:5c:e3:1f:bf:8b:57:6c:5a

"If you trust this host, hit Yes to add the key to PuTTY's cache and
carry on connecting.

"If you want to carry on connecting just once, without adding the key
to the cache, hit No.

"If you do not trust this host, hit Cancel to abandon the connection.
```


RQS Nº 03/2005 - CN
CPMI - CORREIOS
78-15615-01
1203
Fls: 3201
Doc:

"This is a feature of the SSH protocol. It is designed to protect you against a network attack known as *spoofing*: secretly redirecting your connection to a different computer, so that you send your password to the wrong machine. Using this technique, an attacker would be able to learn the password that guards your login account, and could then log in as . . . you and use the account for [his or her] own purposes.

"To prevent this attack, each server has a unique identifying code, called a *host key*. These keys are created in a way that prevents one server from forging another server's key. So if you connect to a server and it sends you a different host key from the one you were expecting, PuTTY can warn you that the server may have been switched and that a spoofing attack might be in progress.

"PuTTY records the host key for each server you connect to, in the Windows Registry. Every time you connect to a server, it checks that the host key presented by the server is the same host key [that was presented] the last time you connected. If it is not, you will see a warning, and you will have the chance to abandon your connection before you type any private information (such as a password) into it."

Handling Rejected SSH Fingerprints

Several situations can cause an SSH fingerprint to be rejected during the authentication process.

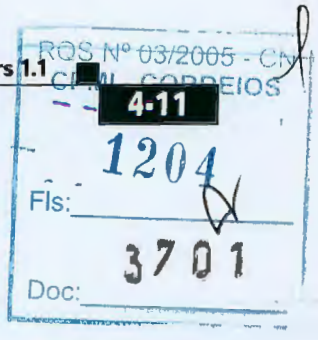
When an SSH fingerprint is rejected, you may see one of the following messages:

- `Error importing configuration files from the sensor: Could not find version in string "Unknown version"`
- `Import failed. Please check the Audit Log for details`

The IDS MC audit log will contain one of the following messages:

- `The SSH fingerprint has changed. Please refer to the documentation for instructions on how to handle rejected fingerprints.`
- *sensorname*: Error executing SSH while importing sensor version from the sensor - Sensor authentication error. Check username, passphrase, and SSH keys.

Note *sensorname* refers to the name of the affected sensor.



E C I
1045
fls
CPL - AC

Caution A rejected SSH fingerprint can indicate a spoofing attack on your network. Benign causes of a rejected SSH fingerprint include a change in a device on your network, such as a network card or an IP address. You can accept the rejected fingerprint, but the security of your network depends on your doing so only after you establish that the rejection is due to benign causes.

To accept a rejected SSH fingerprint, follow these steps:

Step 1 Run the following command:

C:\plink -ssh *userid@ipAddress*

where:

the *userid* is usually **netrangr** for sensor appliances and **ciscoids** for IDSMs.

ipAddress is the IP address to the sensor.

You will see something similar to the following:

```
WARNING -POTENTIAL SECURITY BREACH! The server's host key does not
match the one PuTTY has cached in the registry. This means that either
the server administrator has changed the host key, or you have
actually connected to another computer pretending to be the server.
The new key fingerprint is: 1024
2a:c5:3f:aa:d4:59:82:1d:83:65:58:a1:4e:59:06:bf. If you were expecting
this change and trust the new key, enter "y" to update PuTTY's cache
and continue connecting. If you want to carry on connecting but
without updating the cache, enter "n". If you want to abandon the
connection completely, press Return to cancel. Pressing Return is the
ONLY guaranteed safe choice. Update cached key? (y/n, Return cancels
connection) Connection abandoned.
```

Step 2 Enter **y**.

Step 3 Enter the password of the sensor when prompted.

Step 4 Terminate the session by entering **exit**.

Step 5 Verify that the fingerprint was accepted by running the command again (Steps 1, 3, and 4).

This time you should not get the warning message and update cached key prompt.

Step 6 Verify that you can communicate normally with your sensor by using IDS MC.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
78-15615-01
Fls: 1205
Doc: 3701

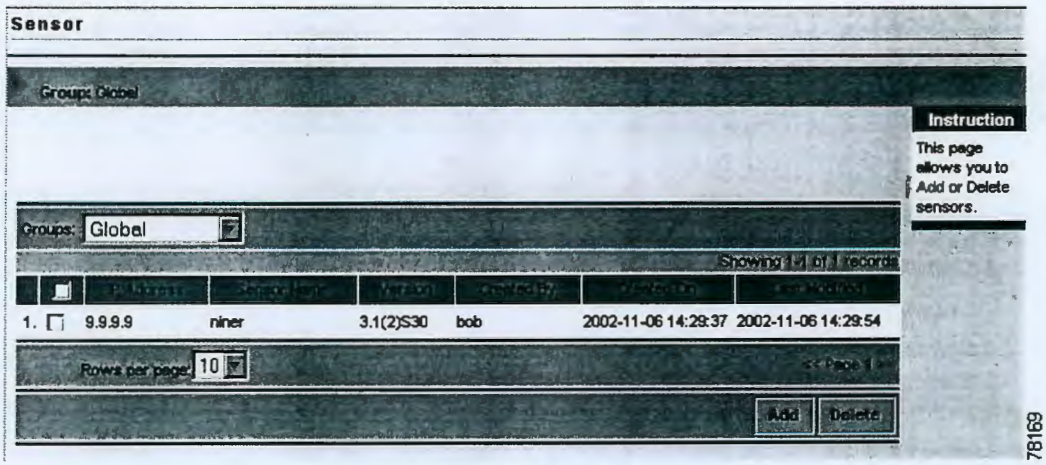
Deleting Sensors from a Sensor Group

You can delete a sensor from any sensor group, including the Global group.

To delete a sensor from a sensor group, follow these steps:

Step 1 Select **Devices > Sensor**.

The Sensor page appears.

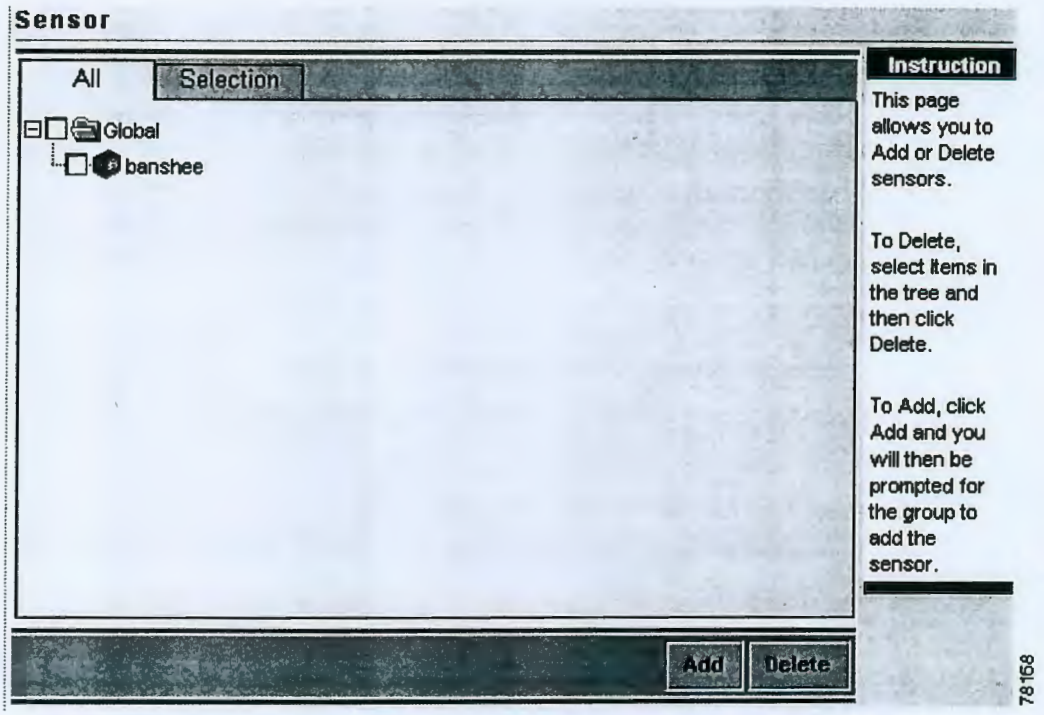


Step 2 In the tree, select the sensor that you want to delete.

Caution If you choose to delete a sensor, IDS MC does not ask you to confirm your choice.

Step 3 Click **Delete**.

The Sensor page appears, updated to show that the sensor was deleted.



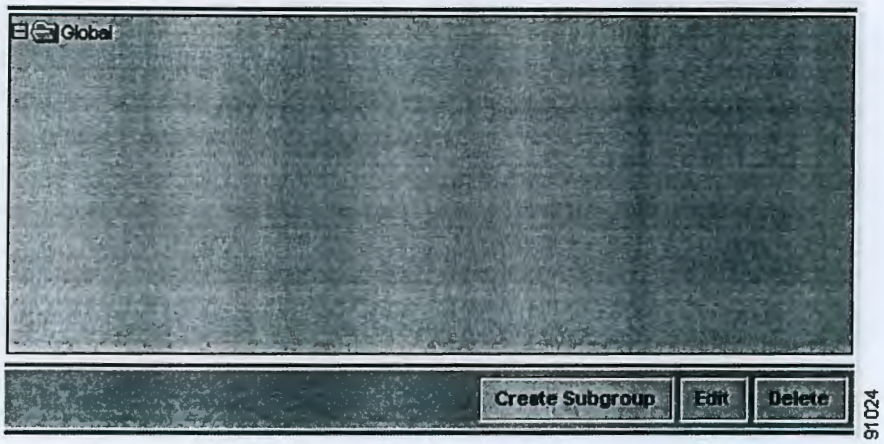
Creating Sensor Subgroups

You can add a subgroup to any sensor group, including the Global group.

To create a sensor subgroup, follow these steps:

Step 1 Select **Devices > Sensor Group**.

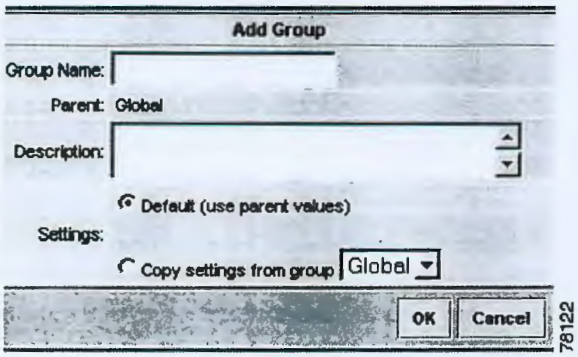
The Sensor Group page appears.



Step 2 In the tree, select the name of the sensor group that you want to add a subgroup to.

Step 3 Click **Create Subgroup**.

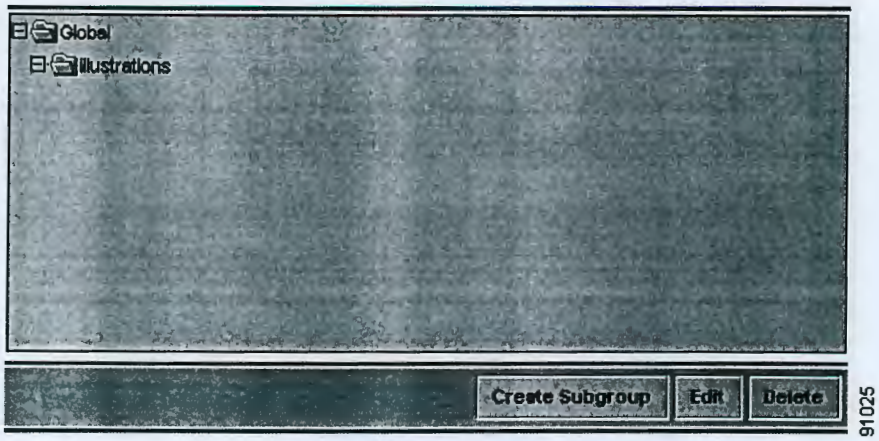
The Add Group page appears.



Step 4 In the Group Name field, enter the name of the subgroup you want to add. Next, select the **Default (use parent values)** radio button, or select the **Copy settings from group** radio button and select the name of the group from the associated list box.

Step 5 Click **OK**.

The Sensor Group page appears, showing the sensor subgroup that you just added.



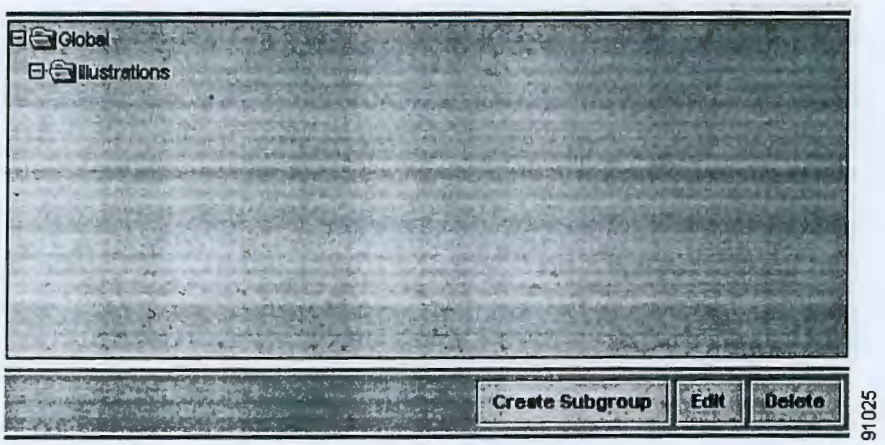
Deleting Sensor Groups

You can delete a subgroup from any sensor group, including the Global group.

To delete a sensor group, follow these steps:

Step 1 Select **Devices > Sensor Group**.

The Sensor Group page appears.



E C I
1.040
Irene
A C

Step 2 In the tree, select the group that you want to delete.

Caution If you choose to delete a sensor group, IDS MC does not ask you to confirm your choice.

Step 3 Click **Delete**.

The Sensor group page appears again, showing the parent of the group you just deleted.

ROS Nº 03/2005 - CN
CEI EIOS
4-17
1210
Fls: 3701
Doc:

4039
CPL

ROS Nº 03/2005 - CN
CPMI - CORREIOS
78-15615-01
1211
Fls:
3791
Doc:

Apêndice CO

RQS Nº 03/2005 - CTN
CPMI - CORREIOS
Fls: 1212
Doc: 3701

Tuning Sensor Signatures Using Policy Override Settings

Some legitimate network activity, such as some types of network virus scanning, has the same characteristics as an actual attack against the network. To prevent these legitimate activities from being reported as an attack, you can tune attack signature settings on a per-device basis. The purpose of tuning is to reduce the number of *false positives*, or detected attacks that are really expected behavior.

Signature tuning falls into three categories: filtering, blocking, and sensing.

Filtering tuning enables you to override the generation of notifications and audit event records by a sensor. Filtering enables you to define specific overrides to the applied sensor signature for that sensor object. The definition of such overrides enables you to tune the sensor to prevent the generation of alarms and audit event records based on false positives, or expected behaviors on your network that satisfy conditions of an attack signature.

In IDSM 2.5.0, 2.5.0, and later versions, you can also define advanced filtering rules that disable the notification of suspicious behavior based on specific traffic flows across the monitored network segment. These refinements are specified in the Filtering panel, and such filter rules disable the generation of alarms and audit event records for traffic originating from or destined to networks and hosts specified in these filter rules.

Blocking tuning enables you to configure a sensor to override the blocking of specific networks for which monitored traffic is studied by the sensor signature running on that sensor.

For example, your sensor signature may have an attack signature set to block the source of the traffic whenever the signature is encountered. However, you may have a network device that generates that signature as part of the device's expected behavior. By tuning the sensor to ignore that attack signature when the source is the trusted network device, you avoid having alarms generated and traffic blocked for that device. However, you still receive alarms and blocking services for that attack signature if it appears in traffic generated from other devices.

Sensing tuning enables you to configure several parameters associated with attack signatures and the sensor device.

For specific signatures that are available to a sensor running IDSM 2.5.0 and later, you can modify how often you are notified about a particular type of attack based on how often the attack occurs and the amount of time that has transpired since the attack was initially detected.

For a sensor running IDSM 2.2.1.5, 2.5.0, 2.5.0, and later, you can specify which IP-based data streams should be studied based on the ability of the sensor to reassemble a fragmented datagram. For a sensor running IDSM 2.5.0 and later, you can also specify which TCP data streams should be studied based on the ability of the sensor to reassemble the entire session. This prevents *false negatives*, or actual attacks that are missed, due to the inability of the sensor to reconstruct the datagram or session.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1213
Fls:
3701
Doc:

E C T
4o037
Doc 1
C P L - A C

Finally, for a sensor running IDSM 2.5.0 and later, you can identify additional ports that should be considered by an attack signature. Some attack signatures are based on a specific port number. These settings allow you to identify additional ports, such as those used by custom TCP services or those used by well-known services that you have reassigned to another port, that should be monitored by those signatures.

Task List for Signature Tuning

You can perform the following tasks on a Sensor node to tune the applied sensor signature.

- "Defining Sensor-Specific Simple Filter Rules to Override Applied Signature Template Rules" on page 2
- "Defining Sensor-Specific Advanced Filter Rules to Override Applied Signature Template Rules" on page 3
- "Defining Global Policy Overrides for the Blocking of Detected Attacks" on page 4
- "Tuning Signatures Applied to a Sensor" on page 4
- "Specifying IP Fragment Reassembly Options for a Sensor" on page 5
- "Specifying TCP Session Reassembly Options for a Sensor" on page 6
- "Identifying the Packet Capture Device of a Sensor" on page 7
- "Identifying Additional Ports Used by Specific Signatures Applied to a Sensor" on page 7

Defining Sensor-Specific Simple Filter Rules to Override Applied Signature Template Rules

A sensor would normally generate a notification and audit event record when it detects a signature pattern. Signature patterns, identified by the signature set applied to a sensor, identify noteworthy patterns in network activity and/or network packet contents. You can define filter rules that exclude specific network packets and activities from generating these notifications and audit event records based on a specific network or host acting as either the source or destination of the network traffic.

To define a simple filtering rule that overrides applied signature template rules, follow these steps:

Step 1 Click the **Sensor** icon ( ) that represents the sensor for which you want to define a simple filter rule, and then click the **Filtering** tab in the View pane.

Result: The Filtering panel appears in the View pane.

Step 2 Click the **Simple Filtering** tab.

Step 3 To define the filter rule settings, click **Add**.

Result: The Create Filter dialog box appears.

Step 4 To specify the primary signature on which the filter rule should be based, select that signature in the Choose a signature to be excluded box.

Result: The Subsignature to be excluded box lists any valid sub-signature.

Step 5 To specify the sub-signature on which this filter rule should be based, select that sub-signature in the Subsignature to be excluded box.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1214
Fls:
3701
Doc:

E C T
4.036
L - AC

Step 6 To specify the network or host address that is excluded from normal signature evaluation, type that address in the IP Address box, and then press **Tab**.

Step 7 To specify the mask for the network or host network that corresponds to the address specified in the IP Address box, type that value in the **Network Mask** box.

Step 8 To specify how the sensor should interpret this rule, select the role of the IP address in the Address Role box.

Step 9 To accept your changes and close the Create Filter dialog box, click **OK**.

Step 10 To define additional simple filter rules, repeat Step 3 through Step 9 for each rule that you want to define.

Step 11 To accept your changes and close the selected panel, click **OK**.

Step 12 To save any changes that you have made, click **Save** on the File menu.

Defining Sensor-Specific Advanced Filter Rules to Override Applied Signature Template Rules

In addition to defining simple filter rules that prevent alarms based on a particular source or destination, you can define advanced filter rules that prevent alarms based on a particular traffic flow that traverses the monitored network segment. In this case, you define a traffic flow based on the source and destination bounding the traffic flow. As you may expect, any flow restriction rules that you have defined on gateway objects in the Network Topology tree will reduce the number of flows that exist between any source and destination that you specify. However, the sensor will prevent alarms based on any valid traffic flows between that source and destination.

To define a filter rule that overrides the applied signature template rules, follow these steps:

Step 1 Click the **Sensor** icon ( ) that represents the sensor for which you want to define an advanced filter rule, and then click the **Filtering** tab in the View pane.

Result: The Filtering panel appears in the View pane.

Step 2 Click the **Advanced Filtering** tab.

Step 3 To define the filter rule settings, click **Add**.

Result: The Create Filter dialog box appears.

Step 4 To specify the primary signature on which the filter rule should be based, select that signature in the Choose a signature to be excluded box.

Result: The Subsignature to be excluded box lists any valid sub-signature.

Step 5 To specify the sub-signature on which this filter rule should be based, select that sub-signature in the Subsignature to be excluded box.

Step 6 To specify the scope of the source for this filter rule, select that type under Source Address.

Step 7 If you selected an option other than Exclude alarms from any IP address, specify values that match the scope type in the boxes that appear under Destination Address.

Step 8 To specify the scope of the destination for this filter rule, select that type under Source Address.

Step 9 If you selected an option other than Exclude alarms to any IP address, specify values that match the scope type in the boxes that appear under Destination Address.

Step 10 To accept your changes and close the Create Filter dialog box, click **OK**.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1215
Fls:
3701
Doc:

E C I
40035
here
A C

Step 11 To define additional advanced filter rules, repeat Step 3 through Step 10 for each rule that you want to define.

Step 12 To accept your changes and close the selected panel, click **OK**.

Step 13 To save any changes that you have made, click **Save** on the File menu.

Defining Global Policy Overrides for the Blocking of Detected Attacks

A sensor can be configured to generate ACL rules and publish them to Managed Devices that block attacks that it detects based on a specific signature pattern. You can prevent specific networks and hosts from ever being blocked by such ACL rules. These networks and hosts are excluded from *all* such rules, despite the settings defined in the signature set applied to the sensor. In other words, these override rules are global for all signatures that the sensor uses to study network traffic.

To specify the networks or hosts that should never be blocked when an attack is detected, follow these steps:

Step 1 Click the **Sensor** icon ( ) that represents the sensor for which you want to define global blocking overrides, and then click the **Blocking** tab in the View pane.

Result: The Blocking panel appears in the View pane.

Step 2 Click the **Never Block Addresses** tab.

Step 3 To define a policy override rule to the block-enabled attack signatures applied to the selected sensor, click **Add**.

Result: A new entry appears in the Never Block Addresses list.

Step 4 To specify the address of the network or host for which you want to override (not apply) any ACL rules that might be generated as the result of the sensor detecting an ongoing attack, type that address in the IP Address box.

Step 5 To specify network mask that corresponds to the address that you specified in the IP Address box, type that value in the Subnet Mask box.

Step 6 For each network or host that you do not want blocked when attacks are detected, repeat Step 3 through Step 5.

Step 7 To accept your changes and close the selected panel, click **OK**.

Step 8 To save any changes that you have made, click **Save** on the File menu.

Tuning Signatures Applied to a Sensor

Specific signatures that are available for a sensor running 2.5.0 IDSM software provide one or two parameters that you can modify to tune how often you are notified about a particular type of attack. This tuning is based on how often an attack occurs and the amount of time that has transpired since the attack was initially detected.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1216
Fls:
3701
Doc:

E C
4.033
CPL - AC

To tune signatures for a sensor, follow these steps:

Step 1 Click the **Sensor** icon ( ) that represents the sensor that you want to tune, and then click the **Sensing** tab in the View pane.

Result: The Sensing panel appears in the View pane.

Step 2 To view the tab where you can specify how often you want to be notified that a specific attack has been detected by the sensor, click the **Signature Tuning Parameters** tab in the Sensing panel.

Step 3 To view the list of editable parameters for a specific signature type, double-click that signature type in the Signature Name box.

Result: The Signature Parameter Editor dialog box appears.

Step 4 To specify how many seconds should transpire after the initial attack that satisfies this signature is detected and before this counter and the threshold value are reset, type that value in the Expiration box.

Step 5 (Optional) To specify the number of times that the sensor can detect the same attack type before issuing an additional notification, type that value in the Threshold box.

Step 6 For each signature that you want to tune, repeat Step 3 through Step 5.

Step 7 To accept your changes and close the selected panel, click **OK**.

Step 8 To save any changes that you have made, click **Save** on the File menu.

Specifying IP Fragment Reassembly Options for a Sensor

For IDSM 2.2.1.5, 2.2.1.6, 2.2.1.7, 2.2.1.8, 2.5.0, 2.5.0, and later, you can specify which IP-based data streams should be studied based on the ability of the sensor to reassemble an entire datagram. In other words, you can specify boundaries that the sensor uses to determine how complete a datagram can be in terms of the reassembly of frames that are transmitted across the physical wire as part of that datagram. The ultimate goal for defining these reassembly settings is to ensure that the sensor does not allocate all its resources to datagrams that cannot be completely reconstructed, either because the sensor missed some frame transmissions or because an attack has been launched that is based on generating random fragmented datagrams.

All reassembly settings work in conjunction to ensure that the sensor has adequate system resources available to study network activities. However, unless you understand the likelihood of fragmented datagrams occurring on your network over a specified period of time, we recommend that you do not modify the default values provided for the IP fragment reassembly settings. However, we recommend two algorithms for determining these values:

- For sensors running IDSM 2.5.0 or later, we recommend that the Maximum Partial Datagrams times the Maximum Fragments Per Datagram remain less than or equal to 5,000.
- For sensors running 2.2.1.5, 2.5.0, or later non-IDSM software versions, we recommend that the Maximum Partial Datagrams times the Maximum Fragments Per Datagram remain less than or equal to 2,000,000.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1217
Doc: 3701

ECT 1.032 CPL - AC

To specify IP fragment reassembly options for a sensor running an applicable IDSM software version, follow these steps:

Step 1 Click the **Sensor** icon ( ) that represents the sensor for which you want to specify IP fragment reassembly options, and then click the **Sensing** tab in the View pane.

Result: The Sensing panel appears in the View pane.

Step 2 To view the tab where you can specify the mapped ports that this sensor should consider, click the **Advanced Sensor Settings** tab in the Sensing panel.

Step 3 To specify that you want the sensor to reassemble IP datagrams, select the **Reassembly Fragments** check box under IP Fragment Reassembly.

Step 4 To specify the maximum number of partial datagrams that the sensor can attempt to reconstruct at one time, type that value in the Maximum Partial Datagrams box.

Step 5 To specify the maximum number of fragments that can be accepted into a single datagram, type that value in the Maximum Fragments Per Datagram box.

Step 6 To specify the maximum number of seconds that can transpire before the sensor stops tracking a particular exchange for which it is trying to reassemble a datagram, type that value in the Fragmented Datagram Timeout box.

Step 7 To accept your changes and close the selected panel, click **OK**.

Step 8 To save any changes that you have made, click **Save** on the File menu.

Specifying TCP Session Reassembly Options for a Sensor

For IDSM 2.5.0 and later, you can specify which TCP data streams should be studied based on the ability of the sensor to reassemble the entire session. Like IP fragment reassembly settings, these settings ensure that valuable system resources are not reserved for sessions that are no longer active.

To specify TCP session reassembly options for a sensor running an applicable IDSM software version, follow these steps:

Step 1 Click the **Sensor** icon ( ) that represents the sensor for which you want to specify TCP session reassembly options, and then click the **Sensing** tab in the View pane.

Result: The Sensing panel appears in the View pane.

Step 2 To view the tab where you can specify the mapped ports that this sensor should consider, click the **Advanced Sensor Settings** tab in the Sensing panel.

Step 3 To specify that the sensor track only sessions for which the three-way handshake is completed, select the **TCP Three Way Handshake** check box.

Step 4 To specify how strict the reassembly requirements are for this sensor when it attempts to reassemble the entire TCP session, select that type in the TCP Strict Reassembly box.

Step 5 To specify the number of seconds that can transpire before the sensor frees the resources allocated to a fully established TCP session, type that value in the TCP Open Establish Timeout box.

Step 6 To specify the number of seconds that can transpire before the sensor frees the resources allocated for an initiated, but not fully established, TCP session, type that value in the TCP Embryonic Timeout box.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1218
Doc: 3701

E C T
4.033
CPL - A

Step 7 To accept your changes and close the selected panel, click **OK**.

Step 8 To save any changes that you have made, click **Save** on the File menu.

Identifying the Packet Capture Device of a Sensor

You can identify the type of packet capture device that a sensor should use to retrieve network packets that it evaluates against the active sensor signature set configured for the sensor. This packet capture device identifies the type of physical layer driver that should be used to capture network packets. In other words, it identifies the type and speed of the physical network that is attached to the monitoring interface installed in the sensor.

Note This option is not available on line card models of the IDS software, such as IDSM 3.0.

To identify the packet capture device of a sensor, follow these steps:

Step 1 Click the **Sensor** icon ( ) that represents the sensor for which you want to identify a packet capture device, and then click the **Sensing** tab in the View pane.

Result: The Sensing panel appears in the View pane.

Step 2 To specify the packet capture device for this sensor, select the correct type in the Packet Capture Device list.

For non-switch-based sensors, you can specify one of the following values:

- **/dev/spwr0**—Identifies the network type that the sensor is studying as an Ethernet network.
- **/dev/mtok**—Identifies the network type that the sensor is studying as one of the older Token Ring networks operating at 4 or 16 MB transfer rates.
- **/dev/mtok36**—Identifies the network type that the sensor is studying as one of the newer Token Ring networks operating at 4, 16, or 100 MB transfer rates.
- **/dev/ptpci0**—Identifies the network type that the sensor is studying as an FDDI network.
- **/dev/iprb0**—Identifies the device name of the NIC interface used for packet capture.
- **auto**—Selects the device that is the default sniffing device on the appliance.

Step 3 To accept your changes and close the selected panel, click **OK**.

Step 4 To save any changes that you have made, click **Save** on the File menu.

Identifying Additional Ports Used by Specific Signatures Applied to a Sensor

For IDSM 2.5 and later, you can specify additional ports that should be considered by advanced attack signatures that study specific network services (identified by the TCP port used by that network service). These port settings enable you to identify any well-known network service ports that you have reassigned on your internal network, and to identify any custom TCP-based services that you run across your internal networks, that you want the sensor to study for specialized attacks that target these network services.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1219
Fls:
3791
Doc:

To identify additional or remapped ports for more extensive evaluation by specific signatures, follow these steps:

Step 1 Click the **Sensor** icon ( ) that represents the sensor for which you want to specify a port, and then click the **Sensing** tab in the View pane.

Result: The Sensing panel appears in the View pane.

Step 2 To view the tab where you can specify the mapped ports that this sensor should consider, click the **Port Mapping** tab in the Sensing panel.

Step 3 To specify additional ports that should be considered by the attack signature that studies for hijacked ports on a TCP-based service, type each port number in the TCP HIJACK Ports box, separating entries with a comma.

Step 4 To specify additional ports that should be considered by the attack signature that studies for TCP-based flood attacks, type each port number in the TCP SYNFLOOD Ports box, separating entries with a comma.

Step 5 To specify additional ports that should be considered by the attack signature that studies for Telnet-based attacks, type each port number in the TCP Telnet Ports box, separating entries with a comma.

Step 6 To specify additional ports that should be considered by the attack signature that studies for HTTP-based attacks, type each port number in the TCP HTTP Ports box, separating entries with a comma.

Step 7 To accept your changes and close the selected panel, click **OK**.

Step 8 To save any changes that you have made, click **Save** on the File menu.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1220
Doc: 3701

Apêndice CP

ROS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1221
3701
Doc:

ISCO SYSTEMS

ECT
14.029
CPL - AC

Data Sheet

CiscoWorks **Security Information Management Solution** 3.1

One of the greatest challenges in enterprise security is managing the flood of alerts generated by a growing number of multivendor security devices and systems. Automation is required to isolate and prioritize the few messages that indicate real security threats.

The key to more effective security automation lies in a software technology known as Security Information Management (SIM). CiscoWorks Security Information Management Solution (CiscoWorks SIMS) is based on technology from netForensics v3.1 and incorporates powerful features for gathering and analyzing the overwhelming amount of security event data that companies are experiencing. Companies can manage their growing security infrastructure and effectively monitor millions of event messages, without additional staff.

With CiscoWorks SIMS, the user has a solution that delivers:

- Complete event monitoring for SAFE and all multivendor security environments
- Real-time event correlation to detect both known and unknown threats
- Advanced visualization for fast and intuitive security monitoring
- Integrated risk assessment to understand the overall vulnerability of any particular asset within the enterprise
- Comprehensive reporting and forensics for all levels of security operations
- Productivity gains and cost reduction

CiscoWorks SIMS delivers these capabilities using the award-winning netForensics software, which is the central component of the solution.

ıetForensics

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1222
3701
Doc:

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement

E C T
4.028
CPL - AC

v3.1 collects, analyzes, and correlates security event information from across the enterprise in a series of four distinct phases: normalization, aggregation, correlation, and visualization.

Normalization and Aggregation

In the normalization and aggregation phases, security events are collected from virtually all intrusion detection systems, firewalls, operating systems, applications, and anti-virus systems and transformed into a common easy-to-understand XML format.

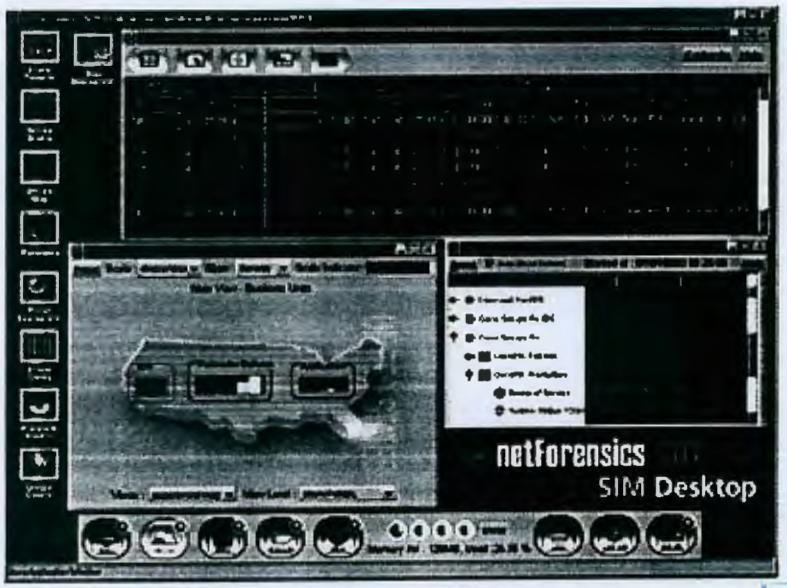
Correlation

Formatted records are then correlated using two distinct yet complementary forms of event correlation. The first is a statistical correlation mechanism that relies upon event categorization and threat scoring to determine the threat potential of security-based anomalies. The second is an optional rules-based correlation feature that separates false positive security alarms from potentially significant security incidents by invoking "time aware" security policy rules for each event received.

With statistical correlation, normalized security events are categorized into security incident types by asset or asset group. Incident types can range from a reconnaissance attack, to a virus attack, to a denial of service attack, to name just a few. For each asset a threat score is continuously computed by combining event severity with asset value to determine an overall measurement of security incident potential. The key advantage is the ability to find those anomalies that may go undetected by a rules-based correlation implementation.

Visualization

netForensics v3.1 displays correlated results on a centralized, real-time console with a graphical, Java-based interface that is powerful, intuitive, and user friendly.



RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1223
Doc: 3701

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

E C T
1 4002 1
Jane
CPL - AC

The Executive Dashboard provides a real-time, enterprise-level view of security trends and the Real-Time Console facilitates fast isolation of security attacks using real-time correlation and analysis capabilities.

Risk Assessment

In security terms, risk assessment involves understanding the overall vulnerability of any particular asset within the enterprise. Risk is commonly defined as the combination of threat, vulnerability, and value, where:

- Threat is any abnormal traffic or activity directed against a system or asset. netForensics scores each threat type, whether it's a port scan or login failure. These scores are then considered in the overall risk calculation.
- Value is the level of importance (perhaps in dollars) of any particular system or asset. The value is a user-defined variable for each asset in the enterprise.
- Vulnerability is the likelihood that a threat will be successful against a system or asset.

The solution combines each of the above to formulate an overall risk score for each asset within the enterprise, with higher scores indicative of higher asset vulnerabilities. The solution produces a Risk Assessment Report that provides the necessary details behind each asset and its associated risk. By understanding the vulnerability of specific assets within an enterprise, companies can strengthen appropriate security policies.

Summary

As securing the enterprise IT infrastructure becomes more challenging, companies must rely on technology to help assimilate the amount of security event information that flows from an ever-increasing number of security devices and systems. In addition, technology must be used to not only aid organizations in reducing the risk of attacks, but also to help accelerate responses when attacks occur. CiscoWorks SIMS increases the effectiveness of existing security teams and thereby helps achieve a real, measurable ROI.

Devices Supported for Monitoring

Table 1 Event Sources and Versions Supported

Application/Device	Version	netForensics Components
Third-party applications	–	Universal Agent
Historical data	See Syslog File Agent	Batch Agent
Arbor PeakFlow DoS	2.1	Agent for Arbor Peakflow
Check Point FireWall-1	NG, 4.1	Agent for Check Point
Cisco IOS® ACL, FW, IDS	12.2, 12.0	Syslog File Agent
Cisco Secure ACS	3.0	Agent for CSACS
Cisco Secure IDS	4.0, 3.1, 2.5, 2.2	CSIDS Agent/Syslog Agent
Cisco Secure PIX®	6.2, 6.1, 6.0, 5.3, 5.2, 5.1, 5.0	Syslog File Agent
Cisco Secure PIX IDS	6.2, 6.1, 6.0, 5.3, 5.2	Syslog File Agent
Cisco VPN Concentrator	3.1, 2.5.2	Syslog File Agent
CyberGuard Firewall	5.1	Agent for CyberGuard

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1224
Fls:
3701
Doc:

14.026

Table 1 Event Sources and Versions Supported

Application/Device	Version	netForensics Components
Dragon Sensor/Squire	5.0 / 1.3.1	Agent for Dragon
Entercept HIDS	2.5, 2.0	Agent for Entercept
ISS RealSecure HIDS/NIDS	6.5, 6.0, 5.5 / 7.0, 6.5, 6.0	Agent for ISS RealSecure
Secure Computing Sidewinder	5.2	Agent for Sidewinder
Snort NIDS	1.8	Agent for Snort
Symantec Enterprise FW/VPN	7.0, 6.5	Agent for Symantec
Symantec ManHunt NIDS	2.2	Enterprise Firewall/VPN
Tripwire NIDS	3.0	Agent for ManHunt
UNIX OS events	Solaris 8/7/6, Linux 7.2/7.1	Agent for Tripwire
Windows events	Windows 2000 Server/Advanced Server	UNIX OS File Agent

The list of supported event sources and versions is frequently updated

System Requirements

Supported Operating Systems

Table 2 lists the supported operating systems for different netForensics components.

Table 2 Quick Lookup for Supported Operating Systems

netForensics Component	Supported Operating System
nF Engine	Red Hat Linux, Solaris 8
nF Master	Red Hat Linux, Solaris 8
nF Provider/Oracle 9i Database	Red Hat Linux, Solaris 8
nF Web Server	Red Hat Linux, Solaris 8
nF Agent for Arbor Peakflow	Red Hat Linux, Solaris 8, Windows
nF Agent for Check Point	Red Hat Linux, Solaris 8, Windows
nF Agent for CSACS	Windows 2000
nF Agent for CSIDS	Red Hat Linux, Solaris 8
nF Agent for CSIDS 4.0	Red Hat Linux, Solaris 8, Windows
nF Agent for CyberGuard	Red Hat Linux, Solaris 8, Windows
nF Agent for Dragon	Red Hat Linux, Solaris 8

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1225
Fls: 3701
Doc:

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

E C
4.025
Fls.
L - A

Table 2 Quick Lookup for Supported Operating Systems

netForensics Component	Supported Operating System
nF Agent for Entercept	Windows 2000
nF Agent for ISS RealSecure	Windows 2000
nF Agent for ManHunt	Red Hat Linux, Solaris 8, Windows
nF Agent for Raptor	Solaris 8, Windows 2000
nF Agent for Sidewinder	Red Hat Linux, Solaris 8, Windows
nF Agent for Snort	Red Hat Linux, Solaris 8
nF Agent for Tripwire	Red Hat Linux, Solaris 8, Windows
nF Agent for Windows	Windows 2000
nF Batch Agent	Red Hat Linux, Solaris 8
nF Batch Agent for Check Point	Red Hat Linux, Solaris 8, Windows
nF Syslog File Agent	Red Hat Linux, Solaris 8, Windows
nF Universal Agents	Red Hat Linux, Solaris 8, Windows
nF UNIX File Agent	Red Hat Linux, Solaris 8

Note: Red Hat Linux 7.1 (Kernel 2.4.9) or Advanced Server only; Windows 2000 Server/Advanced Server (Service Pack 2) only; Solaris on SPARC only

Full Install

Table 3 Minimum System Requirements for Full Install

Component	Requirement
Operating System	See "Supported Operating Systems"
Processor	Linux: Dual Intel Pentium 4 1.5 GHz (server class) Solaris: Dual UltraSPARC-IIi 444 MHz (server class)
Memory	4 GB total system memory
Free disk space	18 GB (see "Disk Partitions" in the netForensics Quick Start Guide)
Storage Device	CD-ROM
Software packages	Linux: Anonymous FTP Server, development libraries, kernel development Solaris 8: See "Solaris Patches and Packages" in the netForensics Quick Start Guide)

Cisco Systems, Inc.
All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1226
Doc: 3701

Ordering Information

CWSIM-3.1-SS-K9	Starter Kit—on Solaris License for monitoring of 30 devices, one master engine, one distributed engine, one Oracle database, agent software for all supported devices
CWSIM-3.1-SL-K9	Starter Kit—on Linux License for monitoring of 30 devices, one master engine, one distributed engine, one Oracle database, agent software for all supported devices
CWSIM-3.1-EN-K9	License for one additional distributed engine on Solaris or Linux
CWSIM-3.1-DS-K9	License for one additional database on Solaris
CWSIM-3.1-DL-K9	License for one additional database on Linux
CWSIM-3.1-ADD20-K9	License for monitoring 20 additional devices

E C T
4.024
Jrent
CPL - AC

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

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Cisco, Cisco Systems, the Cisco Systems logo, Cisco IOS, and PIX are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company.
(0303R)

RQS N 03/2005 - CN
CPMI - CORREIOS
Fls: 1927
Doc: 3701

Apêndice CQ

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1228
Doc: 3701

ECT
4.023
CPL - AC

Overview

CiscoWorks **VPN/Security Management Solution**, Version 2.1

CiscoWorks VPN/Security Management Solution (VMS) is the flagship integrated security management solution from Cisco, and is an integral part of the SAFE blueprint for network security. VMS protects the productivity of organizations, by combining Web-based tools for configuring, monitoring, and troubleshooting enterprise virtual private networks (VPN), 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 VPN to all employees and monitor the VPN service. VMS enables customers to deployment security infrastructures from a small to large environment, using the following multi-faceted scalability features:

- Complete SAFE Coverage
  In order to completely manage a SAFE environment, a network management solution must manage SAFE infrastructure components, support features based upon an appliance or the Cisco IOS® Software, and support the range of management functionality. CiscoWorks VMS is uniquely able to scale across SAFE blueprint components, including firewalls, VPNs, and network- and host-based IDS. 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.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1229
Fls:
3701
Doc:

Cisco Systems, Inc.
All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

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 the 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 enable 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, admin, 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 are managed - not just firewalls but also VPNs, network- and host-based IDS, routers, switches, and so on. 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 IDS, along with event correlation.

Cisco Systems, Inc.
All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1230
Doc: 3701

E C T
Nº 021
June
CPL - AC

CiscoWorks VPN/Security Management Solution (VMS) Components

The following table lists CiscoWorks VMS modules and their functions.

Table 1

	VMS Module	Usage
	Management and Monitoring Centers:	
New!	* Management Center for PIX Firewalls	Configures PIX firewalls
New!	* Management Center for IDS Sensors	Configures Network-based IDS
New!	* Management Center for VPN Routers	Configures VPN routers
New!	* Monitoring Center for Security	Monitors network and host-based IDS events, IOS and PIX syslog
New!	* Auto Update Server	Permits configurations to be pulled from update server
New!	* Common Services	Provides a set of common software and services for the Management Centers
	Cisco Secure Policy Manager	Configures PIX firewall, IOS firewall; and VPN
	Cisco IDS Host Sensor and Console	Configures Host-based IDS, to protect critical servers
	VPN Monitor	Monitors IPSec-based site-to-site and remote access VPN
	Resource Manager Essentials	Provides operational management, such as software distribution, change audit, syslog analysis
	CD One/ CiscoView	Provides graphical device management

The following provides a summary of each CiscoWorks VMS module. For more detailed information, consult the data sheets for the individual modules.

Management and Monitoring Centers

The Management and Monitoring Centers are the newest modules in CiscoWorks VMS and are available exclusively within VMS. These centers include the Management Center for PIX Firewalls, Management Center for IDS Sensors, Management Center for VPN Routers, and Monitoring Center for Security. Common Services provides common functionality across the centers. Auto Update Server is used with the Management Center for PIX Firewalls. These centers supply multifaceted scalability by offering features such as a consistent user experience, auto update, command and control workflow, and role-based access control.

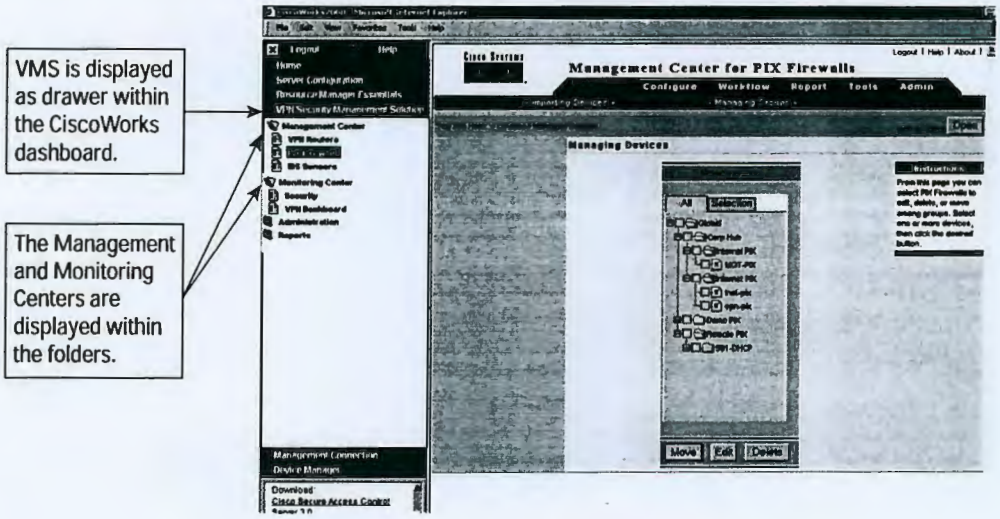
Figure 1 shows CiscoWorks VMS displayed as a "drawer" in the CiscoWorks dashboard. In the drawer are folders for the new Management and Monitoring Centers.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1231
Doc: 3701

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

ECT
CPL - AC
Fls: 1020

Figure 1
CiscoWorks VPN / Security Management Solution



CiscoWorks Management Center for PIX Firewalls

The CiscoWorks Management Center for PIX Firewalls and Auto Update Server enable the large-scale deployment of Cisco PIX Firewalls. The Management Center for PIX Firewalls provides 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 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.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1232
Fls: 3701
Doc:

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

E C T
4.019
CPL - AC

Management Center for IDS Sensors

The Management Center for IDS Sensors is used for the configuration of IDS sensors. Network administrators can use this module to configure network and switch IDS sensors. Many sensors can be quickly configured using group profiles, with the Management Center for IDS Sensors. 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 walk users through common management tasks
- Access to the Network Security Database (NSDB)—Provides meaningful information on alarms for users without IDS security expertise
- Ability to define a hierarchy of sensors containing groups and subgroups; 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

Management Center for VPN Routers

The Management Center for VPN Routers is used for setup and maintenance of large-scale 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) tunnel policies on VPN routers.

Major features include:

- Wizard-based interface for the creation of IKE and VPN tunnel policies
- Hierarchical Inheritance and Smart Rules hierarchy to reflect the organizational and common setup of devices and simplified device management
- IKE-KA (IKE Keep Alive) or generic routing encapsulation (GRE) with Open Shortest Path First (OSPF) and Enhanced Interior Gateway Routing Protocol (EIGRP) for failover routing scenarios.
- Centralized RBAC model allows for centralized management of users and accounts

Monitoring Center for Security

The Monitoring Center for Security provides integrated monitoring to reduce the number of security monitoring consoles, reduce the number of events to monitor, and provide a bigger picture 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 IDS, Switch IDS, Host IDS, 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.

Cisco Systems, Inc.
All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1283
3701
Doc:

ECT
4018
CPL - AC

Auto Update Server

The Auto Update Server is the first product in the industry that allows users to implement a "pull" model for security and PIX operating system management. Auto Update Server permits remote firewall networks with unprecedented scalability. The Auto Update Server allows Cisco PIX firewalls, when used with the Management Center for 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" with Cisco.com and the Cisco PIX Management Center

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.

Cisco Secure Policy Manager (CSPM)

Cisco Secure Policy Manager is a scalable, powerful policy-based security management system for Cisco firewalls and IPSec VPN routers. CSPM 3.1 introduces several features including support for Windows 2000 Server, Windows 2000 Workstation, improved client/server and network object comment. With Cisco Secure Policy Manager, Cisco customers can define, distribute, enforce, and audit network-wide security policies from a central location. CSPM provides the following capabilities:

- Streamlines the tasks of managing complicated network security elements, such as perimeter access control, Network Address Translation (NAT), and IPSec-based VPNs.
- Dramatically simplifies firewall and VPN deployment in enterprise and service provider networks.
- Provides simple graphical user interface (GUI) allows administrators to visually define high-level security policies for multiple Cisco firewalls and VPN routers. These policies can be distributed throughout the network from a central location, thus completely eliminating the costly, time-consuming practice of manually implementing security configurations on a command-by-command and device-by-device basis.
- Provides basic system auditing functions, including real-time alarm notification and a Web-based reporting system.

Cisco IDS Host Sensor and Console

Cisco IDS Host Sensor and Console provides real-time analysis and reaction to network hacking attempts. The Cisco IDS Host Sensor and Console can stop known and unknown attacks, including NIMDA and the Code Red Worm viruses. Cisco IDS Host Sensor and Console can identify an attack and prevent access to critical server resources before any unauthorized transactions occur. Unlike traditional detection products, Cisco IDS Host Sensor and

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1234
Doc: 3701

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Console proactively protects the host by evaluating requests to the operating system and the application programming interface (API) before they are processed. Using a blend of "signature" and behavioral techniques, Cisco IDS Host Sensor and Console stops attacks.

Cisco IDS Host Sensor and Console can intercept and validate software calls made into the operating system and kernel. Calls are matched to a constantly updated database of both defined and generic attack behaviors. If an attack is found, preemptive action is automatically taken to protect the system by referencing a policy that is customized to the environment. Actions ranging from "Log Event" to "Terminate Process" are taken. All activity on the host is seen, and is not impaired by encryption, switched data, or reliance on system log information. The attack database consists of the following types of attack recognition capability:

- Individual attack—Protects against single hacking "exploits" by matching known attack behaviors against activity in the system OS or applications, for example, MDAC and GetAdmin
- Generic attack—Protects against a whole category of hacking "exploits" directed against the operating system and applications, covering unknown and known attacks, for example, Buffer Overflow Exploits, Code Red, and so forth
- Resource protection—Prevents malicious access to system resources, including processes, services, registry keys, password files, authentication mechanisms, and so forth
- Shielding and HTTP protocol protection—Provides additional protection for specific applications, for example, IIS Web Server (requires additional license)

CiscoWorks VPN Monitor

CiscoWorks VPN Monitor is 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 devices throughput problems.
- Enables identification of the devices with 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 key 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.

CiscoWorks Resource Manager Essentials (RME)

CiscoWorks Resource Manager Essentials provides the operational management for the network. CiscoWorks RME allows network managers to perform the following:

- Quickly build a complete network inventory

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1235
Doc: 3701

E C T
4.016
CPL - AC

- 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

CiscoView (CD One)

The CiscoView graphical device management application provides dynamic status, monitoring, and configuration information for the broad range of Cisco internetworking products. CiscoView provides a physical view of a device chassis, with color-coding of modules and ports enabling administrators to check status. Monitoring capabilities display performance and other statistics. Configuration capabilities allow comprehensive changes to devices, provided that users have the proper security access privileges.

CiscoView 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.
- Ability to change device configurations such as IP route, virtual LAN (VLAN), and duplex settings
- Multiuser access to a single CiscoView server in a Web-based application

Server Specifications

Server Hardware

- IBM PC-compatible computer with 1GHz 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
- 10BaseT or faster connection
- 1 GB minimum memory
- 9 GB minimum available disk drive space
- 2 GB virtual memory
- Color monitor with video card capable of 16-bit

Server Operating System

CiscoWorks VMS requires the following operating systems:

- Windows 2000 Professional, Windows 2000 Server (Service Pack 2)
- Sun Solaris 2.7 w Patches:
  - 106327-05 Shared Library Patch for C++
  - 106980-10 Libthread Patch

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1286
Doc: 3701

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

- 107636-03 X Input and Output Method Patch
- 107081-11 Motif 1.2.7 and 2.1.1: Runtime Library Patch
- 108376-03 (1) Open Windows 3.6.1 Xsun Patch

- Sun Solaris 2.8 w/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

Client Requirements

Hardware

- IBM PC-compatible computer with 300-MHz or faster Pentium
- Solaris SPARCstation or Sun Ultra 10

Client Operating System

- Windows 98, Windows NT 4.0, or Windows 2000 Server or Professional Edition with Service Pack 2
- Solaris 2.7, 2.8

Client Browser

- 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.

The Management Center for PIX Firewalls, Management Center for VPN Routers, and Auto Update Server are supported on Internet Explorer 6.0 or 5.5, 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 24x7 access to the Cisco Technical Assistance Center (TAC), full Cisco.com privileges, and software maintenance updates. A Software Application Service 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 on service and support offerings, contact your local sales office.

Ordering Information

CiscoWorks VPN/Security Management Solution (VMS) is available for purchase through normal 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

See http://www.cisco.com/warp/public/cc/pd/wr2k/vpmnso/prodlit/

Email ciscoworks@cisco.com

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

All contents are Copyright © 1992–2002, Cisco Systems, Inc. All rights reserved. Cisco, Cisco IOS, Cisco Systems, the Cisco Systems logo, and PIX are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries. All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0208R)

202977/ETMG, 9/02

RGS MF 03/2005 - CN
CPMI - CORREIOS
Fls: 1237
3701
Doc:

Apêndice CR

RQC Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1238
Data: 3701

ECT 4044 fls. CPL - AC

Cisco Systems

Data Sheet

Cisco Catalyst 6500 Series **Intrusion Detection System** (IDSM-2) Services Module

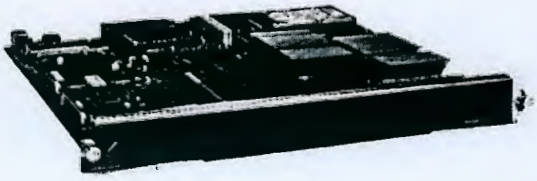
Cisco integrated network security solutions enable organizations to protect productivity gains and reduce operating costs.

The Cisco IDSM-2 is part of the Cisco Intrusion Detection System. It works in concert with the other components to efficiently protect your data 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.

For details on the complete Cisco Intrusion Detection System, go to www.cisco.com/go/ids

Cisco integrated network security solutions enable organizations to protect their connected business assets from threats and increase the operating efficiency of intrusion protection. Among these solutions is the second generation of the Cisco Intrusion Detection System (IDS) module, the IDSM-2, for the widely deployed Cisco Catalyst® chassis. With an installed base in the hundreds of thousands, the Catalyst chassis is a logical platform for additional services such as firewall, virtual private network (VPN) and intrusion detection system (IDS) services. Recognizing the value of this approach, Cisco introduced this second-generation module that provides unique benefits to customers seeking IDS attack protection.

Figure 1
Cisco IDSM-2



Features and Benefits

The Cisco IDSM-2 offers the following features and benefits:

- Cisco is the only vendor to provide an in-switch IDS solution supplying access to the data stream via VLAN access control list (VACL) capture capable of supporting an unlimited number of VLANs
- Transparent operation via passive, promiscuous operation that inspects copies of packets via VACL capture and Switch Port Analyzer/Remote SPAN (RSPAN/SPAN) without exposing the network to performance degradation or downtime if the unit needs maintenance because it is not in the switch-forwarding path

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1239
Doc: 3701

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement

ECT
2003
CPL - AC

- One-rack-unit size takes up only a single slot in the Cisco Catalyst chassis making it an effective platform across all Catalyst chassis, from the 3-slot Catalyst 6503 Switch to the largest chassis available, allowing as many modules to be installed simultaneously as desired providing protection for a greater number of VLANs and traffic
- 500 megabits per second (Mbps) of IDS inspection provides high-speed packet-examination capabilities and allows for more protection of a wider variety of networks and traffic
- Multiple techniques for capture and actions including SPAN/RSPAN as well as VACL capture combined with shunning and TCP resets allows customers to monitor various network segments and traffic while the product provides timely action to mitigate threats
- Uses the same code as the award-winning Cisco IDS network appliances allowing users to standardize on a single management technique and makes installation, training, operation, and support simpler and faster while taking advantage of Cisco IDS comprehensive attack recognition and signature coverage
- Improved management techniques such as support by the Cisco VMS 2.1 security bundle, as well as built-in Cisco IDS Device Manager (IDM) and IDS Event Viewer (IEV) local management capabilities and CLI support make the IDSM-2 easier to manage and more capable of detecting and responding to threats while alerting operators to potential attacks. In addition, the new option makes management of multiple devices across wide and varied networks much simpler

Technical Specifications

Cisco IDSM-2 Part Numbers

WS-SVC-IDS2-BUN-K9

Cisco IDSM-2 Service Part Numbers

CON-xxxx-WS-IDSM2-K9

Service key for "xxxx" in the part number:

- SNT = 8x5xnext business day
- SNTE = 8x5x4 hour service
- SNTP = 24x7x4 hour service
- OS = 8x5xnext business day
- OSE = 8x5x4 hour service onsite
- OSP = 24x7x4 hour service onsite

Form Factor

One rack-unit module uses one slot in the Cisco Catalyst 6500 chassis

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1240
Doc: 3711

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

LEDs and Switches

Single indicator (LED)

- OFF—no power
- YELLOW—booting up/standby
- GREEN—application is running
- RED—module fault located

Shutdown switch used before removing the module from the chassis.

Hot-Swap Requirements

Module shutdown required before removal

Module insertion/removal never affects the Cisco Catalyst switch

Processor

Pentium 1.13 GHz on main board with IXP on the accelerator

Operating System

Red Hat Linux 6.2

Maximum Number of Modules per Chassis

Unlimited per chassis

Traffic Capture Methods

VACL capture

SPAN

RSPAN

Minimum Code Revision

Release 4.0

Features:

- TCP resets
- IP logging
- SME (Signature Micro Engine)
- IDM
- NTP Synchronization
- Local CLI (Command-line Interface)
- Performance enhancements

Cisco Systems, Inc.
All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1241
Doc: 3701

E C T
Folha
AC

Catalyst Supervisor Software Requirements

Catalyst OS 7.5(1) (minimum)

Native Cisco IOS Software Release12.1(19)E

Catalyst Supervisor Hardware Options with IDSM-2

With Catalyst OS 7.5.(1): Supervisor Engine 1A

- Supervisor Engine 1A/PFC2
- Supervisor Engine 1A/MSFC1
- Supervisor Engine 1A/MSFC2
- Supervisor Engine 2
- Supervisor Engine 2/MSFC2

With Native Cisco IOS Software Release 12.1(19)E:

- Supervisor Engine 2/MSFC2

Performance Metrics

600 Mbps with 450-byte packets

Supports up to 5,000 TCP connections per second (new arrivals)

Supports up to 500,000 concurrent connections

100% alarm rate

Catalyst performance not affected by additional VLANs or devices in the Cisco Catalyst chassis

Fabric Enabled

Maximum Number of VLANS (802.1q tagging)

Unlimited

Failover Protection

The IDSM-2 is a passive device that has no disruptive effect on the Cisco Catalyst chassis in the event of failure.

Management

Cisco IDM and IEV are included with IDSM-2.

- Cisco IEV PC-based configuration manager (3 devices)
- Cisco IDM on-board Web browser (1 device)
- Cisco VMS 2.1 with Security Monitor and IDS Management Center v1.1 (minimum 20 devices)

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1242
Doc: 3701

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Physical Dimensions

Occupies any slot in the Catalyst 6000 chassis, and as many IDSM-2 modules can be inserted as desired.

Height: 3.0 cm (1.2 in.)

Width: 35.6 cm (14.4 in.)

Depth: 40.6 cm (16 in.)

Weight: 2.27 kg (5 lb)

Operating Environment

Operating temperature: 0 to 40°C (32 to 104.5°F)

Non-operating temperature: -40 to 70°C (-40 to 158°F)

Operating relative humidity: 10 to 90% (noncondensing)

Non-operating relative humidity: 5 to 95% (noncondensing)

Operating and non-operating altitude: sea level to 3050m (10,000 ft.)

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, VCCI Class A with UTP cables, EN55022 Class B, CISPR22 Class B, AS/NZS 3548 Class B, VCCI Class B with FTP cables

Safety

CE marking according to UL 1950, CSA 22.2 No. 950, EN 60950, IEC 60950, TS 001, AS/NZS 3260

Export Restrictions

Cisco IDSM-2 is classified as a "strong encryption" product and is export restricted. For details see: http://www.cisco.com/wwl/export/crypto/tool/

Additional Information

For information about the Cisco Catalyst 6500 Switch, see http://www.cisco.com/go/6000

For information about the Cisco Secure Intrusion Detection System, see http://www.cisco.com/go/ids/

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

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Cisco, Cisco IOS, Cisco Systems, the Cisco Systems logo, and SMARTnet are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0301R)

RD/LW6099 01/03

ECT 4010 June 1 CPL AC

ROS-N 03/2005 - CN
CPMI - CORREIOS
Fls: 1243
3701
Doc:

Apêndice CS

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1244
Doc: 3791

E C T
4.008
CPL - AC

Caveats

This section includes the following topics:

- Caveat for Operating a 2.2.0 Sensor with a 2.1.1 Director
- Caveats for Operating a 2.2.0 Director with a 2.1.1 Sensor
- Caveats for nrConfigure
- Caveats for the sapd Service
- Caveats for the Security>Advanced>Shunning>Disable Menu Function

Note Refer to the netranger220-readme.txt file bundled with the NetRanger software for last-minute changes and caveats.

Caveat for Operating a 2.2.0 Sensor with a 2.1.1 Director

Operating a 2.2.0 Sensor with a 2.1.1 Director is *not* supported.

Note It is highly recommended that you upgrade to the 2.2.0 Sensor to take advantage of the latest enhancements.

Caveats for Operating a 2.2.0 Director with a 2.1.1 Sensor

If you operate a 2.2.0 Director with a 2.1.1 Sensor, keep the following issues in mind:

- The 2.2.0 Director's nrConfigure adds 2.2.0 tokens to the 2.1.1 Sensor's configuration files. These 2.2.0 tokens will be ignored by the 2.1.1 Sensor.
- The 2.2.0 Director's nrConfigure cannot restart 2.1.1 Sensors due to differences in *postofficed* services. Although the Director does transfer the configuration files, it cannot apply these changes and restart the Sensor. To apply any configuration changes, open a Telnet session to the 2.1.1 Sensor and manually run **nrstop** and **nrstart**.
- If you want to use the 2.2.0 nrConfigure with a 2.1.1 Sensor, you will most likely have to enable the *fileXferd* service on the Sensor.

  To enable this service, Telnet to the Sensor, open the /usr/nr/etc/daemons file in a text editor, either add "nr.fileXferd" to the list of daemons or uncomment the "nr.fileXferd" line, save your changes and exit the editor, and then run **nrstop** and **nrstart** from the command line.
- Certain 2.2.0 Director menu functions have no effect on a 2.1.1 Sensor, including:
  - **Security>Daemons>Restart**
  - **Security>Daemons>Stop**
  - **Security>Daemons>Start**

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1245
Doc: 3701

E C T
1 2007 Jun
C P L - A C

Caveats for nrConfigure

The following are caveats concerning the nrConfigure management tool:

- You can not run more than one copy of the nrConfigure GUI. If this is attempted, error messages will be generated.
- If nrConfigure crashes the first time you start it, you can restart the GUI without further problems.
- nrConfigure may freeze if a remote machine it is trying to configure is not reachable. Make sure that the remote machine is communicating on the network, and try again.

Caveats for the *sapd* Service

If a logfile contains any errors, *sapd* may not load it into the RDBMS, causing *sapd* to fail and generate an error. If this happens, follow these steps:

Step 1 Type `nrstop` to stop the NetRanger services.

Step 2 Type the following command to find the name of the logfile that caused problems:

```
more /usr/nr/var/messages.sapd
```

Step 3 Delete the logfile, mentioned in the messages.sapd file, from the /usr/nr/var/new directory.

Step 4 Type `nrstart` to restart the NetRanger services.

Note When you restart the NetRanger services, it is very likely that you will have duplicate records in your database.

Caveats for the Security>Advanced>Shunning>Disable Menu Function

The **Security>Advanced>Shunning>Disable** menu function keeps the *managed* service from communicating with any routers it is controlling. If you invoke this function and then try to implement manual shunning, your commands will not be passed to the router.

Also, any currently shunned networks or hosts will not be removed from the shun list.

This menu function is normally used to temporarily disable *managed* so you can pass configuration commands to the router safely.

Use the **Security>Advanced>Shunning>Enable** menu function to resume shunning. If you reboot the Sensor, then the temporary disabling of shunning is also reset.

ROS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1246
Doc: 3701

E C T
4.006
CPL - AC

Upgrade Information

This section discusses the following topics:

- Upgrading a Sensor from 2.1.1 to 2.2.0
- Upgrading a Director from 2.1.1 to 2.2.0
- Removed Functionality in NetRanger Version 2.2.0
- Downloading the Sensor and Signature Update

Upgrading a Sensor from 2.1.1 to 2.2.0

If you have an existing 2.1.1 Sensor and would like to upgrade the software to NetRanger version 2.2.0, use Table 1 to guide you in the process.

Table 1 Upgrading a Sensor from 2.1.1 to 2.2.0

Upgrade to 2.2.0, but keep Solaris 2.5.1*		Upgrade to 2.2.0 and upgrade to Solaris 2.6
If you want to keep your configuration files:	**If you want to create new configuration files:**	
1 Refer to Chapter 3, "Installation and Configuration" in the *NetRanger User Guide*. 2 Refer to the "Upgrading Device Management (for Cisco routers)" section of Chapter 3, "Installation and Configuration". 3 Refer to the "Downloading the Sensor and Signature Update" section of these Release Notes. 4 If the Director has also been upgraded and its configuration files changed, use nrConfigure's **Insert Sensor** feature to finalize the configuration.	1 Refer to Chapter 3, "Installation and Configuration" in the *NetRanger User Guide*. 2 Run **sysconfig-sensor** on the Sensor. 3 Run **sysconfig-director** on the Director, and then use nrConfigure's **Add Host** feature to finalize the Sensor upgrade. 4 Refer to the "Downloading the Sensor and Signature Update" section of these Release Notes.	Refer to the "Building a Sensor (Optional)" section of Chapter 3, "Installation and Configuration" in the *NetRanger User Guide*. If you want to upgrade your Sensor hardware, contact your Cisco Sales representative to order a Sensor appliance, which runs on a customized version of Solaris 2.6.

*Solaris 2.5.1 is not year 2000 compliant. Be sure to install the Y2K patches for Solaris 2.5.1.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1247
Fls:
Doc: 3701

Upgrading a Director from 2.1.1 to 2.2.0

If you have an existing 2.1.1 Director and would like to upgrade the software to NetRanger version 2.2.0, use Table 2 to guide you in the process.

Note NetRanger on AIX 4.1.x is no longer supported. Contact a Cisco sales representative to migrate to Solaris or HP-based 2.2.0 Director.

Table 2 Upgrading a Director from 2.1.1 to 2.2.0

If your 2.1.1 Director is:			
Sun Solaris SPARC 2.5.1			HP-UX 10.10
Keep Solaris 2.5.1 and keep configuration files*	**Keep Solaris 2.5.1 and create new configuration files***	**Upgrade to Solaris 2.6**	
If you want to keep your configuration files, refer to Chapter 3, "Installation and Configuration" in the *NetRanger User Guide.*	1 Refer to Chapter 3, "Installation and Configuration" in the *NetRanger User Guide.* 2 Run **sysconfig-director** on the Director. 3 Use nrConfigure to finalize the Director configuration. 4 To upgrade and configure 2.1.1 Sensors, refer to Table 1 of these Release Notes.	1 Refer to the "Uninstalling the Director" section of Chapter 3, "Installation and Configuration" in the *NetRanger User Guide.* 2 Upgrade the operating system to Solaris 2.6. 3 Refer to the "Director Installation and Configuration" section of Chapter 3, "Installation and Configuration" in the *NetRanger User Guide.* 4 To upgrade and configure 2.1.1 Sensors, refer to Table 1 of these Release Notes.	1 Refer to the "Uninstalling the Director" section of Chapter 3, "Installation and Configuration" in the *NetRanger User Guide.* 2 Upgrade the operating system to HP-UX 10.20. 3 Refer to the "Director Installation and Configuration" section of Chapter 3, "Installation and Configuration" in the *NetRanger User Guide.* 4 To upgrade and configure 2.1.1 Sensors, refer to Table 1 of these Release Notes.

*Solaris 2.5.1 is not year 2000 compliant. Be sure to install the Y2K patches for Solaris 2.5.1.

Removed Functionality in NetRanger Version 2.2.0

For NetRanger version 2.2.0, NetView for AIX support on the Director and licensing have both been removed.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1248
Fls:
3701
Doc:

E C T
4.004 Bruno
L - AC

Downloading the Sensor and Signature Update

The Sensor Update contains updates to the signatures list, the Sensor's intrusion detection software, and the Network Security Database (NSDB). This patch is updated periodically.

To obtain the Sensor Update Patch, follow these steps:

Step 1 If you have not already done so, become a CCO member.

To become a CCO member, access the following URL:

`http://www.cisco.com/register/`

and follow the registration instructions.

Step 2 Access the following URL:

`http://www.cisco.com/cgi-bin/tablebuild.pl/nr22-sensor`

Step 3 Log on with your CCO username and password.

Step 4 Download the latest readme and either the Solaris SPARC or Solaris x86 Sensor Update files.

Step 5 For each file, follow the instructions for downloading. You can download via FTP, HTTP, or e-mail.

Step 6 When you have downloaded all the files, use the FTP facility to transfer them to the Sensor.

Step 7 Follow the instructions in the readme file for installing the Sensor update.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1219
Fls:
3701
Doc:

Enhancements

For the 2.2.0 release of NetRanger, the following were a top priority:

- Installation Enhancements
- Support Enhancements
- Usability Enhancements

Installation Enhancements

The following installation enhancement was made for the Sensor:

- **Technician Installation**—The Sensor has been repackaged as a hardware/software appliance with a simplified setup procedure. The technician will first attach the monitoring and control interfaces to the appropriate points on the network. The technician would then temporarily attach a monitor and keyboard to the Sensor and start the initialization script. This script will prompt for several network-related parameters such as IP address, host name, netmask and then several NetRanger-specific parameters such as host and organization. There are a total of seven questions to answer. In a standard deployment, the security office should provide answers for the technician in advance.

On the Director, the following enhancements were made:

- **Simplified install with HP OpenView**—Clearly outlined steps and procedures for configuring OpenView and then installing the NetRanger Director.
- **Interactive Sensor setup wizard**—This new wizard allows the operator to easily connect with a newly installed Sensor. The wizard asks several network-related questions, connects with the new Sensor, and then opens nrConfigure with the default configuration. From this point on the operator can customize the intrusion detection policy and apply it on the new Sensor.
- **Full-featured configuration manager** (see the following section).

Support Enhancements

The following enhancements were made to simplify technical support of NetRanger:

- The Sensor appliances have easy to understand part numbers:
  - NRS-2E (Ethernet)
  - NRS-TR (Token Ring)
  - NRS-2FE (Fast Ethernet)
  - NRS-SFDDI (Single FDDI)
  - NRS-DFDDI (Dual FDDI)
  - Optional -DM suffix on the above part numbers indicates device management option (shunning)
- Device management for all network devices is now bundled in a single option package.
- Sensor migrated to a common platform, with the following characteristics:
  - Single or Dual 400 MHz Processor
  - 100 MHz PCI Bus Monitoring Cards

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1250
3701
Doc:

E C T
4002 June
C P L - A

- **Technology Migration Program**—Cisco provides a Technology Migration Program that allows customers to trade in older hardware for credit against new purchases. There are three 'levels' of trade in. Each level will be given a certain credit for their Sparc-based Sensor and their Pentium-based Sensor. The three levels of trade-in are:
  - — Customers who have purchased WheelGroup products prior to the Cisco acquisition effective April 1, 1998.
  - — Customers that have purchased equipment since the WheelGroup acquisition effective April 1, 1998.
  - — Customers who wish to upgrade from a software-only purchase to the new 2.2.0 appliance.

  These three trade-in deals will be available until April 30, 1999. Contact your Cisco sales representative for details.
- **SmartNet Support** allowing all six levels of Cisco support will be available for the Sensors. Software Application Support with Upgrades will be available for the Director.

Usability Enhancements

The following enhancements were made for product usability:

- The *NetRanger User Guide* was completely reorganized to reflect the new product configuration.
- The nrConfigure tool was changed to offer expanded remote configuration services, including:
  - — Point and click configuration of Sensors
  - — Configuration archival and version control
  - — Sensor recovery tool
  - — Remote signature updates
- The Network Security Database (NSDB), an HTML-based encyclopedia of network security information, is now available.
- Support for Cisco Routers expanded to the following models: Cisco 1600, Cisco 3600, and Cisco 7200.
- Reduced false positive alarm rate by creating a new **RecordOfExcludedNetAddress** token (an enhancement of the previous **RecordOfExcludedAddress** token). The new token allows the user to exclude alarms for entire networks by providing a netmask. The new token also allows the user to exclude alarms based on whether the network address was the source, or destination address for the alarm.

  The **RecordOfExcludedAddress** token is still supported in NetRanger version 2.2.0.
- System error messages about logging, communication, and other NetRanger services, are now graphically represented on the Director's interface. Users can access the Error information in the same way they can access attack Alarm information.
- NetRanger can now log and alarm on policy violations on a Cisco router via the syslogd service. Users can configure the router to send syslogd log files to the Sensor, which can then pass the information to the Director for alarm display.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1251
Doc: 3701

New Signatures

NetRanger version 2.2.0 contains the following new signatures:

- **1103 IP Fragments Overlap**—Some implementations of the TCP/IP IP fragmentation re-assembly code do not properly handle overlapping IP fragments. Teardrop is a widely available attack tool that exploits this vulnerability.
- **2153 Smurf**—This triggers when a large number of ICMP Echo Replies are targeted at a machine. They can be from one or many sources. This will catch the attack known as Smurf, described in the related vulnerability page. Because this attack can come from many sources, automatic shunning of individual hosts is not very effective. If only one network is being used to broadcast the replies, the network can be shunned.
- **2154 Ping of Death Attack**—This triggers when a large number of ICMP Echo Replies are targeted at a machine. They can be from one or many sources. This will catch the attack known as Smurf, described in the related vulnerability page. Because this attack can come from many sources, automatic shunning of individual hosts is not very effective. If only one network is being used to broadcast the replies, the network can be shunned.
- **3001 TCP Port Sweep**—This triggers when a large number of ICMP Echo Replies are targeted at a machine. They can be from one or many sources. This will catch the attack known as Smurf, described in the related vulnerability page. Because this attack can come from many sources, automatic shunning of individual hosts is not very effective. If only one network is being used to broadcast the replies, the network can be shunned.
- **3003 TCP Frag SYN Port Sweep**—This triggers when a large number of ICMP Echo Replies are targeted at a machine. They can be from one or many sources. This will catch the attack known as Smurf, described in the related vulnerability page. Because this attack can come from many sources, automatic shunning of individual hosts is not very effective. If only one network is being used to broadcast the replies, the network can be shunned.
- **3005 TCP FIN Port Sweep**—This triggers when a large number of ICMP Echo Replies are targeted at a machine. They can be from one or many sources. This will catch the attack known as Smurf, described in the related vulnerability page. Because this attack can come from many sources, automatic shunning of individual hosts is not very effective. If only one network is being used to broadcast the replies, the network can be shunned.
- **3006 TCP Frag FIN Port Sweep**—This triggers when a large number of ICMP Echo Replies are targeted at a machine. They can be from one or many sources. This will catch the attack known as Smurf, described in the related vulnerability page. Because this attack can come from many sources, automatic shunning of individual hosts is not very effective. If only one network is being used to broadcast the replies, the network can be shunned.
- **3010 TCP High Port Sweep**—This triggers when a large number of ICMP Echo Replies are targeted at a machine. They can be from one or many sources. This will catch the attack known as Smurf, described in the related vulnerability page. Because this attack can come from many sources, automatic shunning of individual hosts is not very effective. If only one network is being used to broadcast the replies, the network can be shunned.
- **3011 TCP FIN High Port Sweep**—This triggers when a large number of ICMP Echo Replies are targeted at a machine. They can be from one or many sources. This will catch the attack known as Smurf, described in the related vulnerability page. Because this attack can come from many sources, automatic shunning of individual hosts is not very effective. If only one network is being used to broadcast the replies, the network can be shunned.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1252
Doc: 3701

- **3012 TCP Frag FIN High Port Sweep**—This triggers when a large number of ICMP Echo Replies are targeted at a machine. They can be from one or many sources. This will catch the attack known as Smurf, described in the related vulnerability page. Because this attack can come from many sources, automatic shunning of individual hosts is not very effective. If only one network is being used to broadcast the replies, the network can be shunned.
- **3015 TCP Null Port Sweep**—This triggers when a large number of ICMP Echo Replies are targeted at a machine. They can be from one or many sources. This will catch the attack known as Smurf, described in the related vulnerability page. Because this attack can come from many sources, automatic shunning of individual hosts is not very effective. If only one network is being used to broadcast the replies, the network can be shunned.
- **3016 TCP Frag Null Port Sweep**—This triggers when a large number of ICMP Echo Replies are targeted at a machine. They can be from one or many sources. This will catch the attack known as Smurf, described in the related vulnerability page. Because this attack can come from many sources, automatic shunning of individual hosts is not very effective. If only one network is being used to broadcast the replies, the network can be shunned.
- **3020 TCP SYN FIN Port Sweep**—This triggers when a large number of ICMP Echo Replies are targeted at a machine. They can be from one or many sources. This will catch the attack known as Smurf, described in the related vulnerability page. Because this attack can come from many sources, automatic shunning of individual hosts is not very effective. If only one network is being used to broadcast the replies, the network can be shunned.
- **3021 TCP Frag SYN FIN Port Sweep**—This triggers when a large number of ICMP Echo Replies are targeted at a machine. They can be from one or many sources. This will catch the attack known as Smurf, described in the related vulnerability page. Because this attack can come from many sources, automatic shunning of individual hosts is not very effective. If only one network is being used to broadcast the replies, the network can be shunned.
- **3030 TCP SYN Host Sweep**—This triggers when a large number of ICMP Echo Replies are targeted at a machine. They can be from one or many sources. This will catch the attack known as Smurf, described in the related vulnerability page. Because this attack can come from many sources, automatic shunning of individual hosts is not very effective. If only one network is being used to broadcast the replies, the network can be shunned.
- **3031 TCP FRAG SYN Host Sweep**—This triggers when a large number of ICMP Echo Replies are targeted at a machine. They can be from one or many sources. This will catch the attack known as Smurf, described in the related vulnerability page. Because this attack can come from many sources, automatic shunning of individual hosts is not very effective. If only one network is being used to broadcast the replies, the network can be shunned.
- **3032 TCP FIN Host Sweep**—This triggers when a large number of ICMP Echo Replies are targeted at a machine. They can be from one or many sources. This will catch the attack known as Smurf, described in the related vulnerability page. Because this attack can come from many sources, automatic shunning of individual hosts is not very effective. If only one network is being used to broadcast the replies, the network can be shunned.
- **3033 TCP FRAG FIN Host Sweep**—This triggers when a large number of ICMP Echo Replies are targeted at a machine. They can be from one or many sources. This will catch the attack known as Smurf, described in the related vulnerability page. Because this attack can come from many sources, automatic shunning of individual hosts is not very effective. If only one network is being used to broadcast the replies, the network can be shunned.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1253
Doc: 3701

- **3034 TCP NULL Host Sweep**—This triggers when a large number of ICMP Echo Replies are targeted at a machine. They can be from one or many sources. This will catch the attack known as Smurf, described in the related vulnerability page. Because this attack can come from many sources, automatic shunning of individual hosts is not very effective. If only one network is being used to broadcast the replies, the network can be shunned.
- **3035 TCP FRAG NULL Host Sweep**—This triggers when a large number of ICMP Echo Replies are targeted at a machine. They can be from one or many sources. This will catch the attack known as Smurf, described in the related vulnerability page. Because this attack can come from many sources, automatic shunning of individual hosts is not very effective. If only one network is being used to broadcast the replies, the network can be shunned.
- **3036 TCP SYN FIN Host Sweep**—This triggers when a large number of ICMP Echo Replies are targeted at a machine. They can be from one or many sources. This will catch the attack known as Smurf, described in the related vulnerability page. Because this attack can come from many sources, automatic shunning of individual hosts is not very effective. If only one network is being used to broadcast the replies, the network can be shunned.
- **3037 TCP FRAG SYN FIN Host Sweep**—This triggers when a large number of ICMP Echo Replies are targeted at a machine. They can be from one or many sources. This will catch the attack known as Smurf, described in the related vulnerability page. Because this attack can come from many sources, automatic shunning of individual hosts is not very effective. If only one network is being used to broadcast the replies, the network can be shunned.
- **3106 Mail Spam**—Counts number of Rcpt to: lines in a single mail message and alarms after a user-definable maximum has been exceeded (default is 250).
- **3107 Majordomo Execute Attack**—A bug in the Majordomo program will allow remote users to execute arbitrary commands at the privilege level of the server.
- **3108 MIME Overflow Bug**—Fires when an SMTP mail message has a MIME "Content-" field that is excessively long. The token "MimeContentMaxLen" defines the longest valid header length for MIME Content-... Header tokens. It defaults to 200 and is settable to any value greater or equal to 76.
- **3109 Q-Mail Length Crash**—This signature triggers when an attempt is made to pass an overly long command string to a mail server.
- **3221 WWW cgi-viewsource Attack**—Triggers when someone attempts to use the cgi-viewsource script to view files above the HTTP root directory.
- **3222 WWW PHP Log Scripts Read Attack**—Triggers when someone attempts to use the PHP scripts mlog or mylog to view files on a machine.
- **3223 WWW IRIX cgi-handler Attack**—Triggers when someone attempts to use the cgi-handler script to execute commands.
- **3224 HTTP WebGais**—Triggers when someone attempts to use the webgais script to run arbitrary commands.
- **3225 HTTP Gais Websendmail**—Triggers when someone attempts to use the script websendmail to read the password file on a machine.
- **3226 WWW Webdist Bug**—Triggers when an attempt is made to use the webdist program.
- **3227 WWW Htmlscript Bug**—Triggers when an attempt is made to view files above the html root directory.
- **3228 WWW Perfomer Bug**—Triggers when an attempt is made to view files above the html root directory.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1254
Doc: 3701

- **3229 Website Win-C-Sample Buffer Overflow**—This signature triggers when an attempt is made to access the win-c-sample program distributed with WebSite servers.
- **3229 WWW LPerformer Bug**—This signature triggers when an attempt is made to access the win-c-sample program distributed with WebSite servers.
- **3230 Website Uploader**—This signature triggers when an attempt is made to access the uploader program distributed with WebSite servers.
- **3231 Novell convert**—This signature triggers when a user has attempted to use the convert.bas program included with Novell's web server to illegally view files.
- **3232 WWW finger attempt**—This signature triggers when an attempt is made to run the finger.pl program via the HTTP server.
- **3233 WWW count-cgi Overflow**—This signature triggers when an attempt is made to overflow a buffer in the cgi Count program.
- **3251 TCP Hijacking Simplex Mode**—This signature triggers when an attempt is made to overflow a buffer in the cgi Count program.
- **3576 INN Control Message Exploit**—This signature triggers when an attempt is made to execute arbitrary commands via the control message.
- **3400 Sunkill**—Fires when someone attempts to cause the telnetd server to lock up. This will catch the program known as sunkill.
- **3525 IMAP Authenticate Buffer Overflow**—Fires when someone attempts to cause the telnetd server to lock up. This will catch the program known as sunkill.
- **3526 Imap Login Buffer Overflow**—Fires when someone attempts to cause the telnetd server to lock up. This will catch the program known as sunkill.
- **3550 POP Buffer Overflow**—Fires when someone attempts to cause the telnetd server to lock up. This will catch the program known as sunkill.
- **3550 POP Buffer Overflow**—Fires when someone attempts to cause the telnetd server to lock up. This will catch the program known as sunkill.
- **3600 IOS Telnet Buffer Overflow**—Fires when someone attempts to cause the telnetd server to lock up. This will catch the program known as sunkill.
- **3601 IOS Command History Exploit**—This signature triggers on an attempt to force a Cisco router to reveal prior users' command history.
- **4002 UDP Flood**—This triggers when a large number of UDP packets are directed at a host. This will fire when the Pepsi attack is launched across a protected boundary. This signature is also indicative of a UDP port sweep.
- **4051 Snork**—This triggers when a large number of UDP packets are directed at a host. This will fire when the Pepsi attack is launched across a protected boundary. This signature is also indicative of a UDP port sweep.
- **4052 Chargen DoS**—This triggers when a large number of UDP packets are directed at a host. This will fire when the Pepsi attack is launched across a protected boundary. This signature is also indicative of a UDP port sweep.
- **4150 Ascend Denial of Service**—This signature triggers when an attempt has been made to send a maliciously malformed command to an ascend router in an attempt to crash the router.
- **6110 RPC RSTATD Sweep**—Triggers when RPC requests are made to many ports for the RSTATD program.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1255
Fls: 3701
Doc:

- **6111 RPC RUSERSD Sweep**—Triggers when RPC requests are made to many ports for the RUSERSD program.
- **6112 RPC NFS Sweep**—Triggers when RPC requests are made to many ports for the NFS program.
- **6113 RPC MOUNTD Sweep**—Triggers when RPC requests are made to many ports for the MOUNTD program.
- **6114 RPC YPPASSWDD Sweep**—Triggers when RPC requests are made to many ports for the YPPASSWDD program.
- **6115 RPC SELECTION_SVC Sweep**—Triggers when RPC requests are made to many ports for the SELECTION_SVC program.
- **6116 RPC REXD Sweep**—Triggers when RPC requests are made to many ports for the REXD program.
- **6117 RPC STATUS Sweep**—Triggers when RPC requests are made to many ports for the STATUS program.
- **6118 RPC ttdb Sweep**—This signature triggers on an attempt to access the tooltalk database daemon on multiple ports on a single host.
- **6180 rexd Attempt**—Triggers when a call to the rexd program is made. The remote execution daemon is the server responsible for remote program execution. This may be indicative of an attempt to gain unauthorized access to system resources.
- **6190 statd Buffer Overflow**—Triggers when a large statd request is sent. This could be an attempt to overflow a buffer and gain access to system resources.
- **6191 RPC.tooltalk Buffer Overflow**—This signature fires when an attempt is made to overflow an internal buffer in the tooltalk rpc program.
- **6192 RPC mountd Buffer Overflow**—This signature triggers on an attempt to overflow a buffer in the RPC mountd application. This may result in unauthorized access to system resources.

Related Documentation

Use these release notes in conjunction with the following documents:

- *NetRanger User Guide*
- *Regulatory Compliance and Safety Information for NetRanger*

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1250
Doc: 3701

Cisco Connection Online

Cisco Connection Online (CCO) is Cisco Systems' primary, real-time support channel. Maintenance customers and partners can self-register on CCO to obtain additional information and services.

Available 24 hours a day, 7 days a week, CCO provides a wealth of standard and value-added services to Cisco's customers and business partners. CCO services include product information, product documentation, software updates, release notes, technical tips, the Bug Navigator, configuration notes, brochures, descriptions of service offerings, and download access to public and authorized files.

CCO serves a wide variety of users through two interfaces that are updated and enhanced simultaneously: a character-based version and a multimedia version that resides on the World Wide Web (WWW). The character-based CCO supports Zmodem, Kermit, Xmodem, FTP, and Internet e-mail, and it is excellent for quick access to information over lower bandwidths. The WWW version of CCO provides richly formatted documents with photographs, figures, graphics, and video, as well as hyperlinks to related information.

You can access CCO in the following ways:

- WWW: http://www.cisco.com
- WWW: http://www-europe.cisco.com
- WWW: http://www-china.cisco.com
- Telnet: cco.cisco.com
- Modem: From North America, 408 526-8070; from Europe, 33 1 64 46 40 82. Use the following terminal settings: VT100 emulation; databits: 8; parity: none; stop bits: 1; and connection rates up to 28.8 kbps.

For a copy of CCO's Frequently Asked Questions (FAQ), contact cco-help@cisco.com. For additional information, contact cco-team@cisco.com.

Note If you are a network administrator and need personal technical assistance with a Cisco product that is under warranty or covered by a maintenance contract, contact Cisco's Technical Assistance Center (TAC) at 800 553-2447, 408 526-7209, or tac@cisco.com. To obtain general information about Cisco Systems, Cisco products, or upgrades, contact 800 553-6387, 408 526-7208, or cs-rep@cisco.com.

Documentation CD-ROM

Cisco documentation and additional literature are available in a CD-ROM package, which ships with your product. The Documentation CD-ROM, a member of the Cisco Connection Family, is updated monthly. Therefore, it might be more current than printed documentation. To order additional copies of the Documentation CD-ROM, contact your local sales representative or call customer service. The CD-ROM package is available as a single package or as an annual subscription. You can also access Cisco documentation on the World Wide Web at http://www.cisco.com, http://www-china.cisco.com, or http://www-europe.cisco.com.

If you are reading Cisco product documentation on the World Wide Web, you can submit comments electronically. Click **Feedback** in the toolbar and select **Documentation**. After you complete the form, click **Submit** to send it to Cisco. We appreciate your comments.

This document is to be used in conjunction with the documents listed in the "Related Documentation" section.

AccessPath, Any to Any, AtmDirector, the CCIE logo, CD-PAC, Centri, the Cisco Capital logo, *CiscoLink*, the Cisco Management Connection logo, the Cisco Net*Works* logo, the Cisco Powered Network logo, the Cisco Press logo, the Cisco Technologies logo, ClickStart, ControlStream, DAGAZ, Fast Step, FireRunner, IGX, IOS, JumpStart, Kernel Proxy, LoopRunner, MGX, Natural Network Viewer, NetRanger, NetSonar, *Packet*, PIX, Point and Click Internetworking, Policy Builder, RouteStream, Secure Script, SMARTnet, SpeedRunner, Stratm, StreamView, *The Cell*, TrafficDirector, TransPath, VirtualStream, VlanDirector, Workgroup Director, and Workgroup Stack are trademarks; Changing the Way We Work, Live, Play, and Learn, Empowering the Internet Generation, The Internet Economy, and The New Internet Economy are service marks; and BPX, Catalyst, Cisco, Cisco IOS, the Cisco IOS logo, Cisco Systems, the Cisco Systems logo, Enterprise/Solver, EtherChannel, FastHub, ForeSight, FragmentFree, IP/TV, IPX, LightStream, MICA, Phase/IP, StrataSphere, StrataView Plus, and SwitchProbe are registered trademarks of Cisco Systems, Inc. in the U.S. and certain other countries. All other trademarks mentioned in this document are the property of their respective owners. (9810R)

Copyright © 1998, Cisco Systems, Inc.
All rights reserved.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1258
Doc: 3791

Apêndice CT

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1259
Doc: 3701

TECHNICAL BRIEF

Cisco Secure Intrusion Detection System Technical Overview

This document provides a technical overview of the components, capabilities, and architecture of the Cisco Secure Intrusion Detection System, formerly known as NetRanger. Intrusion Detection was developed to extend security visibility into the network and monitor the activity of users while they are on the network. The Cisco Secure Intrusion Detection System (IDS) augments Cisco's end-to-end security solution as a dynamic security component by detecting, responding to, and reporting unauthorized activity from data derived directly from the network.

Cisco Secure Intrusion Detection System Components

The Cisco Secure IDS is a real-time intrusion detection security system that includes the Cisco Secure IDS Sensors, stealthy security appliances that act as "sniffers," and the Cisco Secure IDS Director, a centralized management console. The Director collects incoming Sensor data, translates it, and presents it to security personnel in a map-based and intuitive graphical interface. Users can quickly access additional information about the type of attack from the Director's Network Security Database (NSDB). The Director also allows security personnel to manage the configuration of remote Sensors. And finally, the Director can manage Sensor data by exporting it to third-party relational databases.

Specific Information on Cisco Secure Intrusion Detection System Components

- *Sensor*—The Sensor is a network appliance that combines high reliability with installation and maintenance simplicity. Each network segment monitored requires a dedicated Sensor, including the Internet, intranets, and extranets. The Sensor appliance is optimized for specific data rates and interfaces, such as Ethernet (10BaseT), Fast Ethernet (100BaseT), Token Ring (4 and 16 Mbps), and Fiber Distributed Data Interface (FDDI) (Single or Dual mode). It uses an expert rules-based system engine to distill large volumes of IP network traffic into meaningful security events. It features a unique "three-tiered" attack detection capability to pinpoint unauthorized activity, including, Named attacks, General Category attacks, and Extraordinary attacks. The Sensor can also monitor a router's syslogs for security policy violations, log the security data, "kill" active TCP sessions, and dynamically manage a router's access control lists to shun intruders
- *Director*—The Director provides a map-based graphical interface that provides local, centralized or distributed management for up to hundreds of Sensors across a distributed network. The Director was developed to provide an operations-friendly, point-and-click interface for consistent response to security events. It can also perform other important functions: manage data through third-party tools, access a network security database, remotely monitor and manage Sensors, and send event information to a trouble-ticketing system, pager or e-mail to alert security personnel when security events occur
- *Post Office*—The Post Office is the communications architecture that provides robust, reliable, and efficient communications between Cisco Secure IDS Sensors and Cisco Secure IDS Directors. All communication is supported by a proprietary, connectionless-based protocol that can switch between alternate routes to maintain point-to-point connections

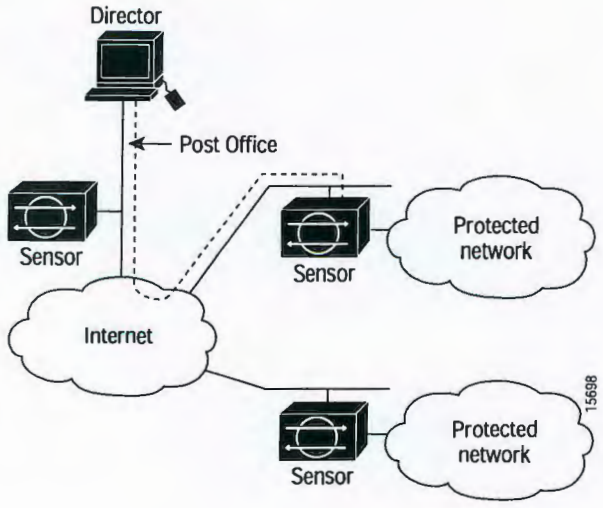
Public
Copyright © 1998 Cisco Systems, Inc. All Rights Reserved.

CISCO SYSTEMS

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1280
Doc: 3701

The relationship between these components is illustrated in Figure 1.

Figure 1 Cisco Secure IDS System Overview



Sensor Capabilities

The capabilities of the Sensor are best described as the following:

- Network sensing
- Attack response
- Device management

Network Sensing

Network sensing involves the real-time intrusion detection monitoring of network packets and syslog data from Cisco routers. The Cisco Secure IDS intrusion detection process captures and analyzes network packets. It not only analyzes single packets, but it retains state on user sessions to detect multiple packet attacks and packet content string matches. The Sensor captures network packets with one of its own interfaces, then reassembles and compares this data against a rule set that indicates typical intrusion activity.

The high performance of the Sensor allows it to scan nearly every packet on a network segment. Therefore, the user is not required to create profiles and omit signatures, which entails constant and extraordinary knowledge of the network to ensure that the correct attack signatures are enabled.

When the Cisco Secure IDS analyzes network data, it looks for patterns of misuse. Patterns can be as simple as an attempt to access a specific port on a specific host, or as complex as sequences of operations distributed across multiple hosts over an arbitrary period of time. The first type of pattern is termed an atomic pattern; the second, a composite pattern.

The Cisco Secure IDS searches for patterns of misuse by examining either the data portion or the header portion of network packets. Content-based attacks derive from the data portion, and context-based attacks derive from the header portion. Table 1 illustrates examples of the types of attacks and patterns that Cisco Secure IDS detects.

Table 1 Types of Patterns and Attacks

	Pattern	
Attack	**Atomic**	**Composite**
Context (header)	• Ping of death • Finger	• Port sweep • SYN attack • TCP hijacking
Content (data)	• MS IE attack • E-mail attacks	Telnet attack

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1201
Doc: 3701

Copyright © 1998 Cisco Systems, Inc. All Rights Reserved.

Another way to look at methodology besides content and context attacks, is via the Cisco Secure IDS's sophisticated and effective "three-tier" attack detection capability. Examples include:

- Named attacks —Single attacks that have specific names or common identities
  - Smurf
  - PHF
  - Land
- General Category attacks—Attacks that keep appearing in new variations with the same basic methodology
  - Impossible IP Packet
  - IP fragmentation
- Extraordinary attacks—Extremely complicated or multi-faceted attacks
  - TCP hijacking
  - E-mail spam

The sophistication of the Cisco Secure IDS's expert system attack detection allows it to detect General Category attacks on-the-fly even as hackers launch new variations to fool security systems. For example there are now many variations of the original named "Land" attack which [illegible] all variations of the general category "Impossible IP Packet." So even as more variations evolve, over time the general category signature will detect them. This attack database is managed, tested, and upgraded by a specialized team that includes some of the industry's most experienced security professionals.

Because a busy network environment can create false positive alarms, the Cisco Secure IDS Sensor can be fine-tuned on a device-by-device basis. For example, if a network management system was constantly creating alarms while pinging the network, the Cisco Secure IDS can be fine-tuned to ignore the specific alarm from that specific address. This capability would not compromise network security because the Cisco Secure IDS would still recognize any other alarms from that address.

Custom Signatures

Users can create custom attack signatures from the Director. These string matching signatures can be used to create a defense for specific new attacks or to detect information unique to the user's environment. For example, the user may be concerned that users are sending unsecured "proprietary" documents across the Internet. A signature can be created to detect all instances of the word "proprietary."

Attack Response

After it detects an attack, a Sensor can respond in the following user-configurable ways:

- Generate an alarm. Alarms are generated by the Sensor, and are typically routed to one or more remote Director systems.
- Log the alarm event. All Sensor log data is written to flat files, which are either event logs or IP session logs.
- Record the session to an IP session log to either gather evidence or an unlawful activity or to record an intruder's knowledge of the network. This capability is commonly used in conjunction with a "fishbowl" or "honeypot" technique where an intruder is vectored into a "safe" network or server that impersonates important applications or information.

Note: IP session logs are written only when a certain event or events occur (for example, a connection request from a specific IP address, or detection of a string such as "Confidential"). When these types of conditions are met, the Sensor can be configured to write every incoming and outgoing packet to an IP session log for a predefined period of time.

- Event logs are continually active, and they can contain alarm, command, and error entries.

Note: Both event and IP session information can be logged locally on a Sensor system as well as remotely on Director systems; exactly what information is sent and where it is sent depends on how each Sensor system is configured.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1263
Fls:
3701
Doc:

Copyright © 1998 Cisco Systems, Inc. All Rights Reserved.

- "Kill" the session by resetting TCP connections. The Sensor can reset individual TCP connections after an attack to eliminate the threat. Communication between all other connections continues, thereby decreasing the likelihood of denial-of-service problems that can occur after shunning TCP-based attacks.
- Shun the attack and deny network access. This option includes using the Device Management feature described in the next section. Shunning an attack involves reconfiguration and reloading of the security filters or access control list (ACL) of a Cisco router. This type of automated response by the Sensor should be configured only for attack signatures with a low probability of false positive detection, such as an unambiguous SATAN attack. A shun can also be manually executed from the Director system in response to an attack or suspicious activity.

Note: Shunning requires careful review before it is deployed, whether as a set of automatic rules or operational guidelines for staff. In case an alarm is generated from a critical host or network, the Cisco Secure IDS can be configured to never shun that host or network. This safety mechanism prevents denial-of-service attacks using the Cisco Secure IDS infrastructure.

Device Management

Device management is a product feature that allows the Sensor to dynamically reconfigure the ACLs on a Cisco router to shun the source of an attack in real time. This capability greatly enhances the ability of the Sensor to secure a network from external and internal threats and gives the user extensive reach to stop misuse network-wide.

The Sensor (illustrated in Figure 1-2) uses one of its network interface cards (NICs) to monitor traffic, and another interface to execute commands and communicate with the router. This scenario allows the Sensor to dynamically update the ACLs on the router in response to traffic that enters the network.

Currently, the Sensor is packaged to support Ethernet, Fast Ethernet, Token Ring, and FDDI monitoring interfaces. It is important that the Sensor be used on a promiscuous mode hub and not on a switched hub. If used on a switched hub, the Sensor can only "see" traffic if the switch supports a monitoring or Switched Port Analyzer (SPAN) port. The command interface is always Ethernet.

Router Syslog Monitoring

With over two million Cisco routers installed around the world, the ACL is the most prevalent security mechanism used on networks. Because they are used to enforce policy, the Cisco Secure IDS Sensor can monitor their system logs for policy violations and send alarms to the Director.

Figure 2 Example Sensor-Network Device Deployment

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1263
Fls:
3701
Doc:

Copyright © 1998 Cisco Systems, Inc. All Rights Reserved.

Director Capabilities

The Director provides centralized command and control over the Sensors in an organization's network. The software-based Director includes installation wizards for fast and complication-free installation. From a capabilities perspective, a Director monitors and manages Sensors, collects and analyzes network security data, downloads new attack signatures, and facilitates user operation. The Director does not feature onboard reporting, because this could compromise its ability to process critical attack information; consequently, data is exported to third-party database and reporting systems.

Network Security Database

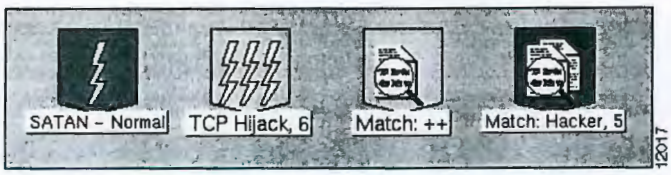
The Director uses a map-based, color icon method of displaying alarms, allowing the user to drill down and pinpoint the exact alarm and analyze its threat potential. The HTML-based Network Security Database is available on the Director to provide an attack description, possible countermeasures, and can be customized to include the specific response procedures for the organization. This scenario ensures response consistency despite staff and shift changes.

Sensor Monitoring

The Director displays real-time security information sent to it by Sensors. This information is presented via icons drawn on one or more network security maps.

Director arranges icons into hierarchical security maps based on the Network Node Management (NNM) user interface of HP OpenView. Users can double-click on an icon to view the next lower "submap" in the hierarchy. The bottom layer of the submap hierarchy contains Alarm and Error icons, as illustrated in Figure 3.

Figure 3 Sample Director Alarm Icons



Each icon, whether it represents a Machine, an Application, or an Alarm, has a state, which is expressed in the form of textual and graphical attributes. The most visible indication of an icon's state is its color. These colors represent states and alarm levels, which are defined in Table 2.

Table 2 Icon Color, State, and Default Alarm Level

Icon Color	Icon State	Default Alarm Level
Green	Normal	1
Yellow	Marginal	2–3
Red	Critical	4–5

An icon's color propagates upward through the submap hierarchy. For instance, an Alarm icon that is defined as "Critical" is red. The application that generates a red alarm will turn red to match the Alarm; in turn, the machine that owns the Application will also turn red.

Every icon in a Director hierarchy also possesses textual attributes, most of which are accessible by the user. Each type of icon (Machine, Application, Alarm) has a different set of attributes.

Sensor Management

The Director can remotely manage the configuration of services on a Sensor. The application responsible for Sensor management is nrConfigure. The signature configuration dialog of nrConfigure is shown in Figure 1-4. Configuring signatures on a remote Sensor is a key method for securing a network with the Cisco Secure IDS.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1204
Doc 3701

Public
Copyright © 1998 Cisco Systems, Inc. All Rights Reserved.

13989

Sensor Installation

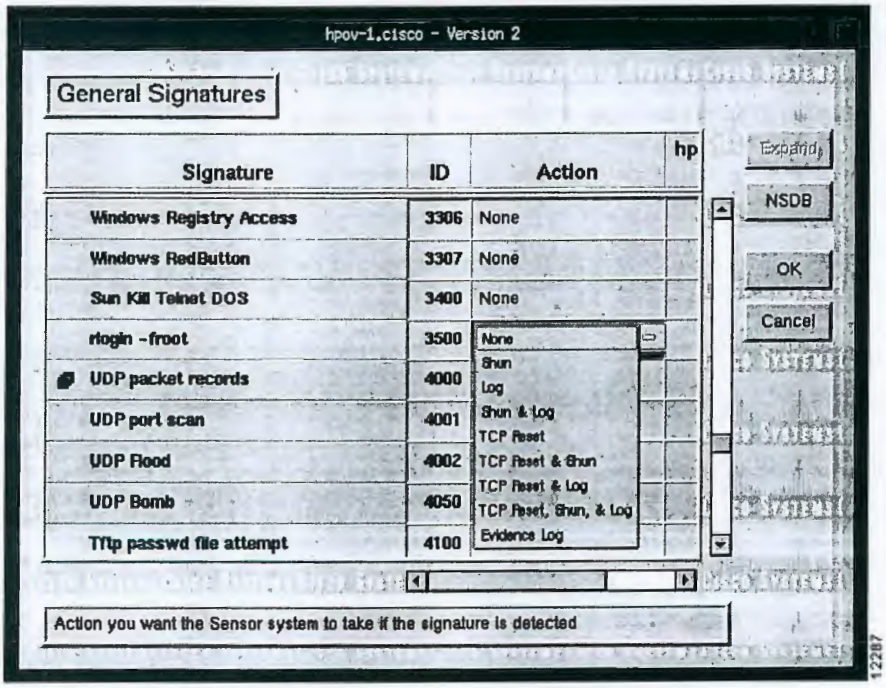
The Sensor can be quickly and easily installed by a technician and requires no special training. The Sensor is simply attached to the network and the technician enters basic network addressing information via a laptop computer. The Director is then programmed to look for the Sensor. When it establishes communications, the Sensor first downloads its configuration, which is stored in the Director's Configuration Librarian as SENSOR X, VERSION 1. The Sensor then begins exporting alarms and can receive commands from the Director. As the Sensor is reconfigured, each configuration is given a new version number.

The Sensor does not require specialized software licensing, and can be moved around the network at will.

Sensor Recovery

If a Sensor goes out of service, an alarm is immediately displayed by the Director. If it is determined that the Sensor has failed, a replacement Sensor can be delivered to the location and quickly installed. The configuration can be quickly restored via the Configuration Librarian in nrConfigure.

Figure 4 Managing Sensor Actions with nrConfigure



nrConfigure is a Java-based tool used for remote Sensor configuration and configuration file management. With this tool, a user can change the configuration files on a remote Sensor, and also manage versions of those configuration files. This functionality allows users to keep current as well as past configurations. At any point, nrConfigure allows a user to "roll back" a Sensor to a previous configuration. Users can easily replicate a specific configuration to one or more Sensors without having to individually configure each one.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1265
Doc: 3701

Copyright © 1998 Cisco Systems, Inc. All Rights Reserved.

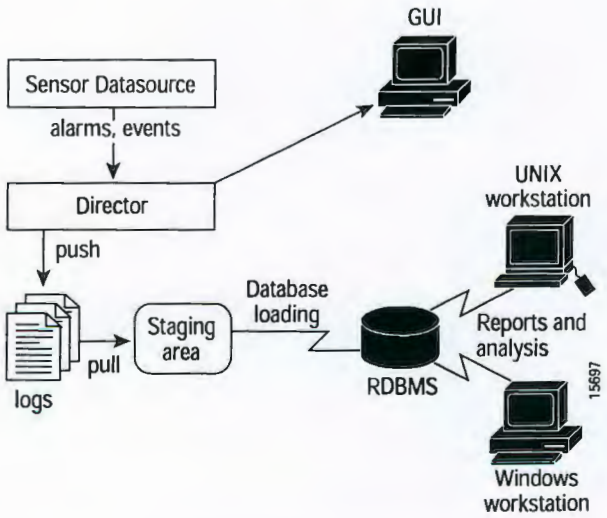
For any given version of a Sensor's configuration, nrConfigure allows users to make changes to the following types of information:

- Communications
- Data management
- Device management
- Director forwarding
- Event processing
- Intrusion detection
- System files
- Collection of Sensor Data

The Director can collect and stage Sensor data using a simple push-pull mechanism: the Cisco Secure IDS writes (pushes) the data into flat files, then stages (pulls) the data into a database. The entire process is illustrated in Figure 5.

Writing to intermediate flat files in this manner provides levels of fault tolerance and performance that cannot be achieved when writing directly to a database. Data throughput in a distributed application such as the Cisco Secure IDS is constrained only by the weakest link in the system. With Cisco Secure IDS's data collection process, data collection is not dependent on (or affected by) database availability or perf nce fluctuations.

Figure 5 Sensor Data Collection



The ctor currently ships with drivers for Oracle and Remedy. However, these drivers can also be configured to write to other databases, such as Sybase and Informix. Example scripts shipped with the Director show how the native bulk load tools of a database can be easily integrated into the Cisco Secure IDS.

The Director also includes a configurable file management capability that automatically archives event and IP logs, either on a Sensor or a Director. Sample file management profiles are provided for both Sensor and Director configurations.

Analysis of Sensor Data

The Director can also analyze Sensor data using third-party tools that provide relational database management, report writing, file management, and trouble-ticketing functionality.

As a foundation for custom reports, the Director includes a set of Sequenced Query Language (SQL) queries that can be easily customized or integrated into any third-party tools.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1266
Doc: 3701

Copyright © 1998 Cisco Systems, Inc. All Rights Reserved.

The third-party data analysis tools can be configured to support individual queries as well as predefined reports. For example, these tools can easily generate reports showing the following:

- All alarms of levels 4 and 5 occurring in the last 30 days
- A graph of Web server activity over the last 24 hours
- A table of all events in the last 30 days in order of increasing alarm levels

Support for User-Defined Actions

The Director can generate user-defined actions. A common action is to notify staff members via e-mail messages or feed data onto third-party devices, such as a printer or database management system. Support for multiple action scripts is also provided.

Post Office Capabilities

Cisco Secure IDS services and hosts communicate with one another through the Post Office, including communication between services on the same host as well as those across a network. All communication is based on a unique three-part address with Organization, Host, and Application identifiers, which uniquely identify each Cisco Secure IDS node.

The proprietary three-part addressing scheme of the Cisco Secure IDS has the following characteristics:

- It can be layered on top of existing network protocols.
- It allows for fault-tolerant connectivity across heterogeneous network architectures.
- It addresses a much larger domain than the current 32-bit IP protocol.

The three-part addressing scheme of the Cisco Secure IDS also serves as the basis for a point-to-point protocol that allows for up to 255 alternate routes between two hosts. This alternate routing protocol automatically switches to the next route whenever the current route fails. It also uses a system heartbeat to detect when a connection to the preferred route can be reestablished. A system error message is generated (and logged) whenever a connection goes down, and any packets that were lost during the state transition are resent.

Another feature that complements alternate routing is the ability to build hierarchies of Sensor and Director systems through the use of message propagation. Instead of broadcasting events from a Sensor onto multiple hosts, information can be sent to a single Director, which can then propagate packets onto other platforms defined in its local configuration files. Sensors can propagate messages to more than one Director, thereby ensuring fault-tolerant communication.

Figure 6 illustrates this concept through a simple hierarchy of Director machines.

In addition to providing performance benefits and fault tolerance, distribution hierarchies can simplify system management. For example, local Director machines might be responsible for monitoring from 9 A.M. to 5 P.M. and then transfer control onto a central Director every evening.

Figure 6 Director Hierarchy Based on Message Propagation

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1267
Fls:
3791
Doc:

Copyright © 1998 Cisco Systems, Inc. All Rights Reserved.

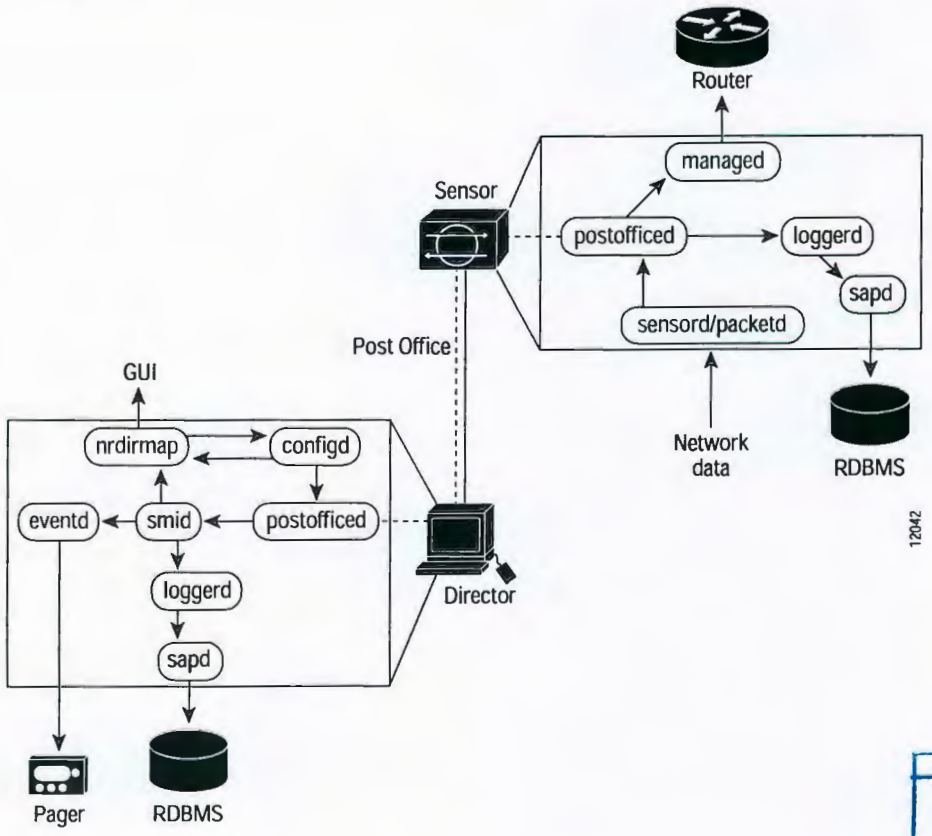
Cisco Secure Intrusion Detection System Architecture

Sensors, Directors, and the Post Office each have separate operational components, called daemons or services. Because each major Cisco Secure IDS function is accomplished by a separate service, the results are a security system that is fast, durable, and scalable.

The services, illustrated in Figure 7, are defined as follows:

- *sensord/packetd*—Both of these services provide intrusion detection. sensord is used when a Sensor is cooperating with a network device that supports copy_to/log_to functions (which sends copies of captured packets to the Sensor); packetd is used when the Sensor itself is capturing packets directly from the network.
- *Loggerd*—This service is the logging facility of the Cisco Secure IDS. It is responsible for writing error, command, and alarm entries to log files on the Sensor.
- *sapd* —This service provides data and file management. It is responsible for moving log files to database staging areas, off-line archives, and other routine processes to prevent file systems from filling up.
- *Postofficed*—This service handles communication between Cisco Secure IDS services and Cisco Secure IDS nodes. As illustrated in Figure 7, when sensord detects unauthorized activity, it signals postofficed; postofficed is then responsible for telling loggerd to start logging, alerting smid on the Director, and communicating orders to a router if the attack is to be shunned.
- *sm*—This service runs on the Director only, and is responsible for translating Sensor data into meaningful information for nrdirmap.
- *nrdirmap*—This service is responsible for displaying various symbols that represent machines, collections of machines, applications, alarms, and errors on the Director graphical interface.
- *eventd*—This service is responsible for maintaining user-defined event notification processes. Users can define what kinds of alarms or other events launch an action, usually an e-mail or pager notification.
- *configd*—This service provides a mechanism through which nrdirmap can interface with other services such as postofficed, sensord, and managed. In other words, commands on the graphical interface can be executed via the underlying configd service.

Figure 7 Cisco Secure IDS 2.2.0 Architecture



Public
Copyright © 1998 Cisco Systems, Inc. All Rights Reserved.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1268
Doc: 3701

Cisco Systems

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

European Headquarters
Cisco Systems Europe s.a.r.l.
Parc Evolic, Batiment L1/L2
16 Avenue du Quebec
Villebon, BP 706
91961 Courtaboeuf Cedex
France
http://www-europe.cisco.com
Tel: 33 1 69 18 61 00
Fax: 33 1 69 28 83 26

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Headquarters
Nihon Cisco Systems K.K.
Fuji Building, 9th Floor
3-2-3 Marunouchi
Chiyoda-ku, Tokyo 100
Japan
http://www.cisco.com
Tel: 81 3 5219 6250
Fax: 81 3 5219 6001

Cisco Systems has more than 200 offices in the following countries. Addresses, phone numbers, and fax numbers are listed on the

Cisco Connection Online Web site at http://www.cisco.com/offices.

Argentina • Australia • Austria • Belgium • Brazil • Canada • Chile • China • Colombia • Costa Rica • Croatia • Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong • 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 • Singapore Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela

Copyright © 1998 Cisco Systems, Inc. All rights reserved. Printed in USA. NetRanger is a trademark; Cisco, Cisco Systems, and the Cisco Systems logo are registered trademarks of Cisco Systems, Inc. in the U.S. and certain other countries. All other trademarks mentioned in this document are the property of their respective owners. (9810R)

Apêndice CU

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1270
Doc: 3701

CHAPTER 6

Configuring Administrative Control Communications

Before Cisco Secure Policy Manager can manage a Managed Device, you must configure a Policy Distribution Point to communicate with that Managed Device. In addition, you must provide the administrative passwords and other connection information required to actually manage that Managed Device. This chapter focuses on the constraints that you must consider when defining the settings that enable this administrative traffic to flow across your network.

The following sections describe device-specific settings that you must configure before you can manage a Managed Device, as well as those settings that enable the generation and distribution of audit event messages, in the form of syslog data streams.

Policy Distribution Panel

The Policy Distribution Point panel is primarily an informational panel. It represents the Policy Distribution Point residing on a Cisco Secure Policy Manager server. The role of the Policy Distribution Point is critical to the operation of the security system. From this panel, you can disable the Policy Distribution Point, which prevents this host from generating and distributing commands to any Managed Devices residing on your network. You can also enable previously disabled Policy Distribution Points.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1271
Doc: 3701

Learn More About Policy Distribution Points

Within the Cisco Secure Policy Manager system, the Policy Distribution Point plays a critical role. This component performs the following tasks:

- It discovers a subset of the existing configuration settings for the Managed Devices that it controls.
- It accepts the intermediate network policies from the Policy Server Point.
- It acts as a distributed component of the security system that *generates* command sets. It translates the intermediate policies into device-specific command sets for each Managed Device that it controls.
- It acts as a distributed component of the security system that *publishes* command sets. It publishes the appropriate generated device-specific command set to each Managed Device that it controls.
- It acts as a distributed component of the security system that *provides feedback* to the system and user. It queries each Managed Device that it controls about the device's status with respect to publishing and discovery attempts, including successes and problems during a publishing attempt and connection problems during discovery.

These command sets can be published securely using secure protocols, such as PIX Secure Telnet, or the Policy Distribution Point can use an IPSec tunnel to publish the command sets securely to the Managed Devices that it controls.

Because each type of Managed Device has its own *control* agent within the Policy Distribution Point component, a Policy Distribution Point can control more than one Managed Device type and multiple Managed Devices of a specific type. For example, a single Policy Distribution Point can control three IOS routers and four PIX Firewalls if configured to do so. However, in scenarios where a Policy Distribution Point controls more than one Managed Device, it is critical to consider the placement of the primary server or secondary server on which the Policy Distribution Point resides in relation to the Managed Devices that you want it to control. In addition, some Managed Devices have restrictions with respect to which interface(s) in the device can be used to configure them. In such cases, considering the limitations of the Managed Device can also help you determine the correct placement of Policy Distribution Points on your network.

Because the Policy Distribution Point component is installed on all Cisco Secure Policy Manager hosts, you can always alter the way that you want to configure your distributed security system. Just as you can enable or disable a Policy

Monitor Point for use as a valid option in configuring your security system, you can also enable or disable a Policy Distribution Point. Cisco Secure Policy Manager uses the selection of a Policy Distribution Point to ensure that the communication between a selected Policy Distribution Point and the Managed Devices that it controls are permitted. The security policies and IPSec Tunnel Groups that enable these communications are automatically generated and maintained by Cisco Secure Policy Manager.

Guidelines for Deploying and Selecting a Policy Distribution Point

The design of your security system deployment should focus on reducing the time required to generate and publish command sets to the Managed Devices residing on your network, as the publishing act temporarily prevents the Managed Device from passing traffic. In addition, this design should focus on quickly monitoring data streams about network activity and detecting and notifying the proper personnel of potential security problems.

You can resolve many issues that can affect your ability to deploy network security policies to Managed Devices by carefully planning the placement of Policy Distribution Points within your network. The benefits of careful planning and placement include the following:

- Administrative connections to the Managed Device are guaranteed by the security policies that are generated by Cisco Secure Policy Manager to enable these connections.
- Connections to Managed Devices are not lost because of changes to the active command set during the publishing operation.
- Distribution of the command sets to the Managed Devices is more secure and the distribution time is reduced.

Because you can have more than one Policy Distribution Point on your network, you must consider the selection of a Policy Distribution Point on a per-Managed Device basis. The best way to make this selection is to understand the scenarios that can be problematic with regard to command distribution and to understand the effects of device-specific changes that you want to make after the initial deployment.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1272
Doc: 3701

Selecting a Policy Distribution Point

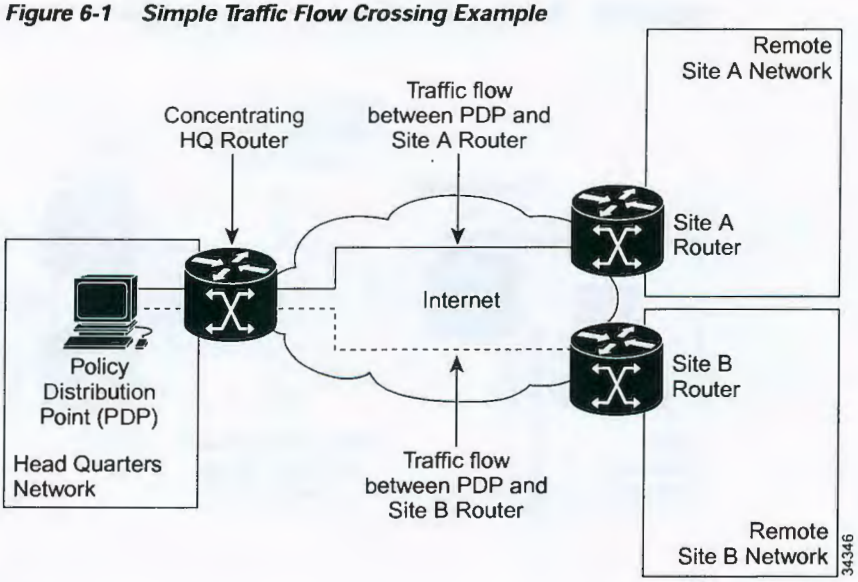
You should not arbitrarily select the Policy Distribution Point to control a Managed Device. When you define global network policies, it is possible in scenarios where you are controlling multiple Managed Devices to effect changes that temporarily disable the required communications between the Policy Distribution Point and one or more Managed Devices that it controls.

The first thing to determine when selecting a Policy Distribution Point is the traffic flows for the communications that occur between the Policy Distribution Point and all the Managed Devices that it controls. Next, you must consider the other Policy Distribution Points on your network and their required traffic flows. It is imperative that these traffic flows do not cross.

When such traffic flows cross, they can only cross at a gateway object, which is referred to as a *concentrating gateway object* for the remainder of this discussion. If that concentrating gateway object is a Managed Device, it identifies a possible point of failure in the publishing of command sets, as the policies managing that gateway object can be altered as well. Since concentrating gateway objects represent points along the path between one or more Managed Devices and a Policy Distribution Point, these concentrating gateway objects can potentially be updated before the farther Managed Devices are provided with command sets that reflect the changes on the concentrating gateway object. This case is most likely to occur if you have enabled automatic publishing of the command sets by selecting Automatic under Command Approval in the Options dialog box (available on the Tools menu) or in the Command panel of a specific Managed Device.

The following example presents a simple topology that identifies crossing traffic flows from a single Policy Distribution Point.

Figure 6-1 Simple Traffic Flow Crossing Example

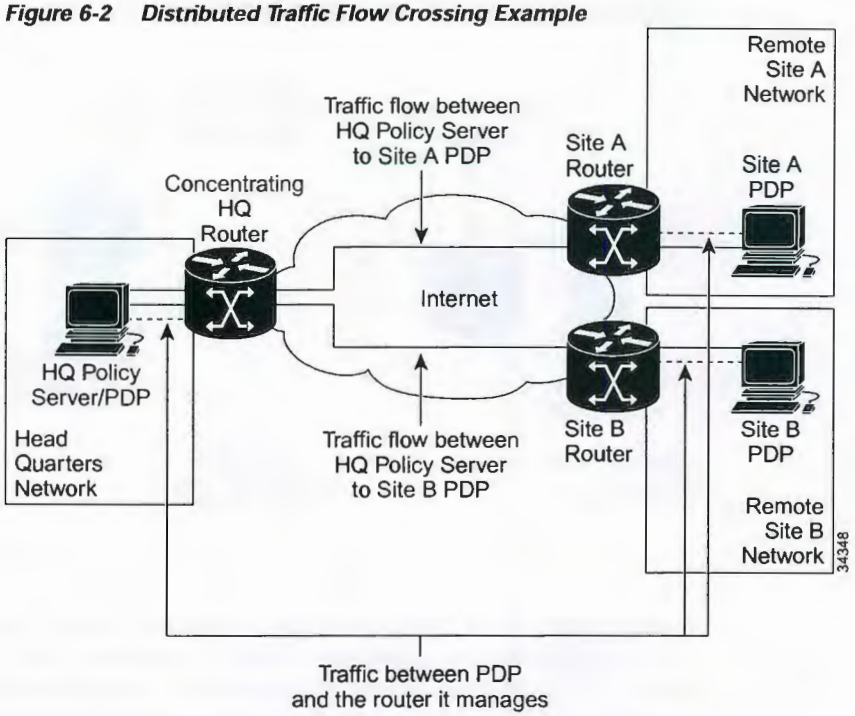


In this example, the HQ Router acts as a concentrating gateway object when the Policy Distribution Point attempts to publish the generated command sets to the routers on Site A or Site B. Therefore, the only way to ensure that the traffic flows to the Site A and Site B routers are not broken is to publish to those outermost Managed Devices *before* you publish to the HQ Router.

You can also have crossing traffic flows in topological scenarios that have multiple Policy Distribution Points, as illustrated in the following example.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1273
Doc: 3701

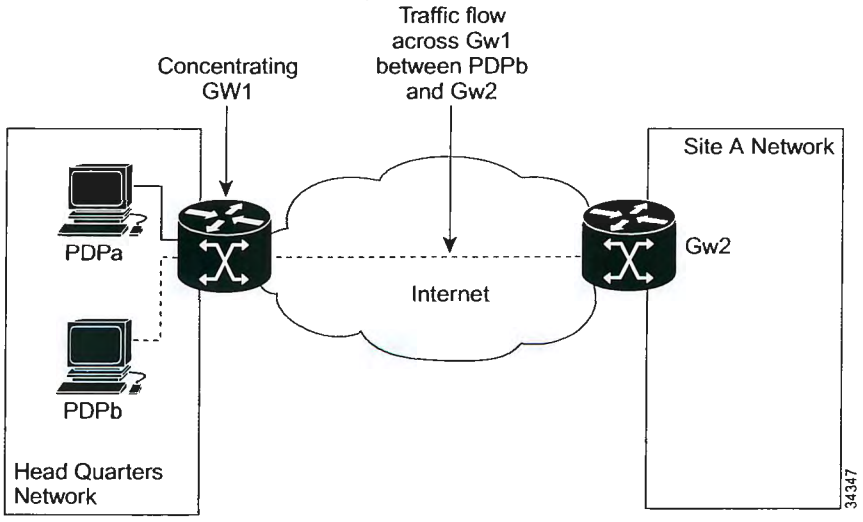
Figure 6-2 Distributed Traffic Flow Crossing Example



In this case, the traffic flows that you must protect against being terminated are the traffic flows between the primary servers and the secondary servers of Cisco Secure Policy Manager. This problem only arises in scenarios where you have a distributed installation type for Cisco Secure Policy Manager.

A third, and unsupported, traffic flow crossing also involves a distributed installation scenario. In this case, two or more Policy Distribution Points publish to different Managed Devices, and one of the Managed Devices acts as the concentrating gateway object. The following example illustrates this crossing traffic flow.

Figure 6-3 Distribution of Two Policy Distribution Points Across a Concentrating Managed Device



In such cases, Cisco Secure Policy Manager does not support the intelligent synchronization of command distribution across such concentrating gateway objects. In this configuration, PDPa is oblivious to the needs of PDPb during the time that PDPb is publishing the generated command set for Gw2. As a result, PDPa could publish command sets that disrupt or disable the ability for PDPb to publish command sets to Gw2.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1274
3701
Doc:

Avoiding Losses of Connectivity between a Policy Distribution Point and a Managed Device

When defining your network topology and making modifications to the Managed Devices on that network, you must also consider the device-specific settings that affect the traffic flows. The following device-specific settings are of particular concern:

- **Administrative interface and IP address changes on a Managed Device.** If you specify a different administrative interface or modify the IP address used for the administrative interface at any time after your initial configuration, you must define a special security policy that enables the old interface to be used to issue the entire command set (because the connection may be lost in the middle once the new interface is configured).
- **Administrative password.** If you specify a different administrative password, such as an enable password, using the Pending Commands option in the Command panel on a Managed Device or using a third-party administrative interface, you must make the corresponding change in the Control panel of the Managed Device in the GUI client before you can publish a new command set to the Managed Device.
- **IP address changes on Cisco Secure Policy Manager hosts.** Any time that you change the IP address used by a host running some component of Cisco Secure Policy Manager or select a different Policy Distribution Point to control a Managed Device (which is effectively a change in the IP address used to manage the Managed Device), you jeopardize the ability of the system to actually publish the command sets to a Managed Device. These addresses are best defined as static IP addresses (not leased via DHCP), and they are best left unmodified.

  If you do modify the IP address that Cisco Secure Policy Manager uses to publish the commands to a Managed Device (the address in the Control panel) or if you select a different Policy Distribution Point to manage a specific Managed Device, you must define an intermediate security policy that allows the network service selected in the Control panel to enable both the old and the new IP addresses. Otherwise, the connection to the Managed Device is broken while the Policy Distribution Point is publishing the command set that changes from the old address to the new address.

- **Routing rules.**Cisco Secure Policy Manager automatically derives the routing rules required to ensure that traffic flows between Policy Distribution Points and the Managed Devices that they manage. If you override a derived routing rule or disable the generation of derived routing rules, you can accidentally cut off the routes used by these required communications.
- **Path restriction rules** (flow restrictions). You must ensure that the traffic flows required for Policy Distribution Point-to-Managed Device communications are not prevented in either direction by a path restriction rule defined on a gateway object.
- **Address hiding and static translation rules on Managed Devices.** You should never define an address hiding rule for a Policy Distribution Point. If you must translate the IP address of a Policy Distribution Point, you must define a one-to-one static translation rule. Any changes to the one-to-one mapping rule have the same effect as modifying the IP address of the Policy Distribution Point. Therefore, you must define a temporary security policy for each Managed Device managed by the Policy Distribution Point that allows that Managed Device to accept the network service used to publish command sets from both the old and new alias addresses of the Policy Distribution Point. For more information on defining these temporary security policies, see the "Learn More About Managed Devices" section on page 6-12.
- **Address hiding and static translation rules on unmanaged gateway objects.** Mapping rules defined on unmanaged gateway objects along a traffic flow between a Managed Device and its Policy Distribution Point translate the IP addresses used to manage the communication and disrupt the traffic flow. You cannot define address translation rules that affect the addresses used for such communications. Therefore, we strongly recommend that you do not define a mapping rule (or have any form of NAT) defined on an unmanaged gateway object residing between your Policy Distribution Point host and the Managed Devices that it manages.

  Unmanaged gateway objects that reside between any Managed Devices and Policy Distribution Points within your Network Topology tree definition cannot have any form of address translation being performed on these unmanaged gateway objects if either the Managed Device or Policy Distribution Point resides upstream from them. Unmanaged gateway objects matching this configuration will guarantee that the generated command sets derived for gateway objects that are managed by Cisco Secure Policy Manager are incorrect. These network services include the network services required for Policy Distribution Point-to-Managed Device communications.

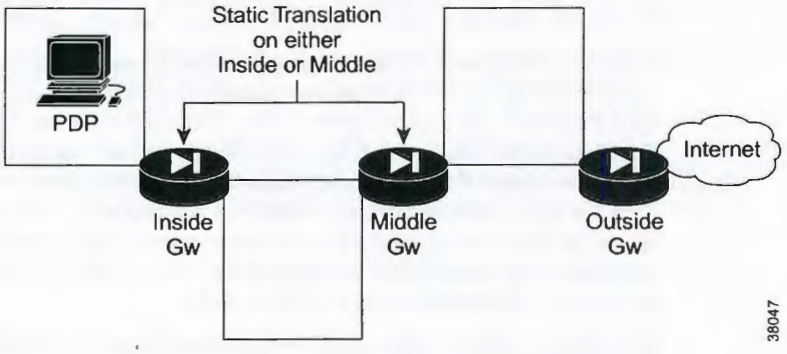
RQS Nº 03/2005 - CN
CPMI - CORREIOS
1275
Fls:
Doc: 3701

Publishing Generated Command Sets: Ordering Restrictions Example

You can construct network topologies for which you should not use automatic command distribution. The problem lies in the order that command sets are downloaded to various Managed Devices. The problem occurs when a Cisco Secure Policy Manager server attempts to publish command sets to an external Managed Device from behind an internal Managed Device that translates the server's real address. In some cases, the automatically downloaded command sets can fail and prevent the download of generated command sets to some Managed Devices in the topology.

The following example assumes that you have a network topology in which you have defined three Cisco Secure PIX Firewalls (called Outside Gw, Middle Gw, and Inside Gw in this example) and that the Cisco Secure Policy Manager host (PDP) that distributes command sets to each of these Managed Devices resides upstream from Inside Gw. Now assume that you have defined a mapping rule on either Middle Gw or Inside Gw that performs a one-to-one static translation for the addresses of PDP.

Figure 6-4 Three PIX Firewall Distribution Ordering Restriction Example



Warning **You cannot define address hiding rules that hide Cisco Secure Policy Manager hosts from the Managed Devices that they are expected to manage. Defining such rules guarantees that the device-specific command sets cannot be published to the Managed Devices for which Cisco Secure Policy Manager is responsible.**

In this case, if you distribute the commands to Inside Gw or Middle Gw before you distribute them to Outside Gw, Outside Gw becomes unreachable by PDP. Even though the command set generated for Outside Gw understands the static translation rule, the command set to be replaced does not. Therefore, Outside Gw does not know to allow administrative updates from the translated PDP address.

Note The automatic command distribution to Outside Gw fails only when a change to the mapping rules occurs on Inside Gw or Middle Gw. In other words, it can occur when you add, delete, or modify an existing mapping rule for the Cisco Secure Policy Manager host, PDP. Once you use the manual distribution method to change the mapping rules, you can return to the automatic distribution method until a similar change occurs.

In this example, if the address of the PDP is not translated on any Managed Devices or it is translated only on Outside Gw, automatic updates would work fine, because in that case order does not matter.

Enabling/Disabling the Policy Distribution Point

You can enable or disable a Policy Distribution Point that resides on a primary or secondary server. If you enable a previously disabled Policy Distribution Point, you can use it to generate and publish device-specific command sets to the Managed Devices on your network. However, if you disable a Policy Distribution Point, you can no longer use it to generate and publish device-specific command sets to any Managed Devices on your network. In fact, a disabled Policy Distribution Point is not a valid option for the Policy Distribution Point box in the Control panel of the Managed Devices that are managed by Cisco Secure Policy Manager.

To enable or disable the Policy Distribution Point, follow these steps:

Step 1 Right-click the **primary server** icon or the **secondary server** icon that represents the server on which the Policy Monitor Point is running.

Step 2 To view the **Policy Distribution** panel, point to **Properties**, and then click **Policy Distribution** on the shortcut menu.

Result: The Policy Distribution panel appears in the View pane.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1276
Doc: 3701

Step 3 To change the availability of the Policy Distribution Point running on this host, select or clear the **Disabled** box under **General Settings**.

When this box is selected, the Policy Distribution Point is disabled. When the box is cleared, the Policy Distribution Point can be used to generate and publish command sets to the Managed Devices residing on your network.

Step 4 To accept your changes and close the selected panel, click **OK**.

Step 5 To save any changes that you have made, click **Save** on the **File** menu.

Control Panel

From the Control panel, you can identify those hosts running the Policy Distribution Point, Policy Monitor Point, and syslog servers that you want to use to control and monitor this Managed Device. You can specify the Telnet and enable passwords required to administer this Managed Device. You can also view the settings for the associated network service (TCP or UDP port) that administrative clients use to communicate with the Managed Device and whether you want to use an IPSec tunnel to encrypt such communications.

Caution If you modify the IP address that Cisco Secure Policy Manager uses to publish the commands to a Managed Device (the address in the Control panel), you must define an intermediate security policy to allow the network service selected on the Control panel to that enables both the old and the new IP addresses. Otherwise, the connection to the Managed Device is broken while the Policy Distribution Point is publishing the command set that changes from the old address to the new address.

Learn More About Managed Devices

The Control panel organizes the configuration settings about communications that occur between a Managed Device and two other types of network objects: Cisco Secure Policy Manager hosts and third-party syslog servers. This Managed Device represents a gateway object over which you have administrative control, and one on which you can use Cisco Secure Policy Manager to enforce global

network policies. A Managed Device accepts commands generated by a Managed Device control agent that resides on either the primary server or a secondary server on which the Policy Distribution Point for the Managed Device resides.

The first setting that you can review is the network service used for communications between the Managed Device and a Cisco Secure Policy Manager host that is acting as the Policy Distribution Point for this Managed Device. By default, for a PIX Firewall, this network service is PIX Secure Telnet, defined as TCP port 1467. For an IOS router, this network service is Telnet, defined as TCP port 23. For an IDS sensor, this network service is postoffice, defined as UDP port 45000. Currently, you cannot reconfigure the port settings associated with these network services. In addition, these network services are the only network services that are valid for downloading network policies to the respective Managed Device.

As part of this general setting, you can specify which IP address, and therefore which interface, should be used to accept communication requests from Cisco Secure Policy Manager hosts.

Note For Managed Devices based on the 4.2.4, 4.2.5, and 4.4.1 versions of the PIX Firewall software, you must specify a Policy Distribution Point that resides upstream from the "inside" interface. This Policy Distribution Point server does not have to reside on the same network, but for security purposes, it must be reachable from the inside interface. In addition, you can use only the PIX Secure Firewall network service to manage the PIX Firewall.

For Managed Devices based on the 5.0 and 5.1 versions of the PIX Firewall software, you must specify a Policy Distribution Point that resides upstream from any interface, except for the "outside" interface. This Policy Distribution Point server does not have to reside on the same network, but for security purposes, it must be reachable from a non-outside interface. In addition, you can use only the PIX Secure Firewall network service to manage the PIX Firewall.

For Managed Devices based on the 5.1 version of the PIX Firewall software, you can specify a Policy Distribution Point server that resides downstream from the "outside" interface using PIX Secure Telnet that is passed through an IPSec tunnel. In other words, you must define an IPSec Tunnel Group definition that has the Policy Distribution Point and the outside interface address of the PIX Firewall as peers in that definition.

ROS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1287
Doc: 3701

In any release of the product, Cisco Secure Policy Manager does not support the basic Telnet network service for management of the PIX Firewall.

Next you must specify which Cisco Secure Policy Manager host is responsible for generating and publishing the command sets to the Managed Device. In addition to specifying which host will publish the generated command sets to the Managed Device, you can specify whether you want to encrypt all communications that occur between the Managed Device and the host acting as its Policy Distribution Point. You can define an IPSec tunnel between the Policy Distribution Point and the Managed Device, as well as specify the IPSec Tunnel Template you want to use when defining the IPSec Tunnel Group that supports this communication.

However, modifying the settings of an IPSec Tunnel Group used for Policy Distribution Point-to-Managed Device communications can disable the communications. For more information on how to modify such an IPSec Tunnel Group, see the "Notes for Defining Policy Distribution Point-to-Managed Device Tunnels" section on page 6-14. For guidance on selecting the Policy Distribution Point that will control a Managed Device, see the "Learn More About Policy Distribution Points" section on page 6-2.

Notes for Defining Policy Distribution Point-to-Managed Device Tunnels

The tunnel group that supports this communication, as well as the security policy abstract that enables the tunnel and permits communications between the Managed Device and the Cisco Secure Policy Manager host acting as its Policy Distribution Point, is automatically created and applied to the Cisco Secure Policy Manager host within the Cisco System Folder of the IPSec Tunnel Groups and Security Policy Enforcement branches under the Network Policy tree.

We also recommend that you never reuse an IPSec template that is used for the Policy Distribution Point-to-Managed Device traffic. Instead, you should make copies of the template before you modify any settings. This recommendation exists because if you change any properties of this IPSec template, it would result in the generation of a modified IPSec bootstrap command set for any Managed Devices managed by the Policy Distribution Point for which you modified the template properties.

If you do modify the template used to manage a Managed Device, all attempts to publish the generated command sets to the Managed Devices will fail and the following warning message will appear for each affected Managed Device in the System Inconsistencies panel when you perform a Save and Update operation:

- (ire) Action(s) required: Change bootstrap settings with new PDP-PEP IPSec tunnel settings, then click Approve to publish. (signature=#)

To resolve this warning message, you must manually update the IPSec bootstrap settings for each affected Managed Device (using a non-Cisco Secure Policy Manager administrative interface). After these settings are updated for each affected Managed Device, these warning messages will be resolved when the command sets are published to each Managed Device.

If you accidentally modify this IPSec template, you can perform a Reset operation. You will still receive the warning message identified above; however, this message will be resolved when you publish the generated command set to the affected Managed Device, because the IPSec bootstrap settings have already been defined to resolve this issue.

As a general rule, any modifications to either tunnel peer affects the IPSec bootstrap settings, and, therefore, requires that you manually update the IPSec bootstrap settings for the Managed Device acting as a peer in the generated IPSec Tunnel Group definition under the Cisco Systems Folder of the IPSec Tunnel Groups branch. Examples of such changes include the following:

- Specifying a new Policy Distribution Point for the Managed Device
- Specifying a new IP address for use as the management address for a Managed Device
- Defining a one-to-one static translation for the Policy Distribution Point
- Modifying any interface settings of the Managed Device

Understanding the Policy Distribution Point's Role When Controlling the Managed Device

This section explains the role of the Policy Distribution Point in more detail, and it provides guidelines for selecting the Policy Distribution Point to use for a particular Managed Device. This choice should not be made arbitrarily, because it can affect the ability of Cisco Secure Policy Manager to publish command sets to multiple Managed Devices.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1278
Doc: 3701

Caution If you modify the IP address that Cisco Secure Policy Manager uses to publish the commands to a Managed Device (the address in the Control panel), you must define an intermediate security policy that allows the network service selected in the Control panel to enable both the old and the new IP addresses. Otherwise, the connection to the Managed Device is broken while the Policy Distribution Point is publishing the command set that changes from the old address to the new address. However, you must be especially careful when using mapping rules on the intermediate Managed Devices. For more information on the allowed uses of mapping rules on intermediate Managed Devices, see the "Caution: Using Mapping Rules that Effect Policy Distribution Point Traffic" section on page 6-18.

By default, all communications between the Policy Distribution Point and a PIX Firewall are encrypted using the PIX Secure Telnet network service. However, you can use an IPSec tunnel to encrypt all communications between a Policy Distribution Point and any Managed Device, assuming that the Managed Device supports IPSec tunnels and that the Cisco Secure Policy Manager host acting as the Policy Distribution Point has the Cisco Secure VPN Client software installed and operational. However, if you chose to enable IPSec tunnels for these communications, all administrative clients that you use to connect to the Managed Device must also support IPSec. In addition, you will have to define an IPSec Tunnel Group for those communications and define security policies that permit IPSec-based communications between each administrative client and the Managed Device.

The Control panel also enables you to specify those passwords that are required to administer the Managed Device. For each PIX Firewall, you must specify the enable password. For an IOS router, you must specify both the Telnet and enable passwords. The Policy Distribution Point uses these passwords to authenticate to the Managed Devices before it downloads the derived network policies.

Note You cannot change these passwords in the Control panel. Instead, you must use the Pending Commands option in the Command panel to change these passwords.

While each Managed Device has only a single Policy Distribution Point, you can specify that you want one or more remote hosts to receive the syslog data streams generated by the Managed Device. These hosts can either be a Cisco Secure

Policy Manager host that is acting as a Policy Monitor Point or another host that runs a syslog server. You can select only one Policy Monitor Point, and as many syslog servers as you want.

Note The current release of Cisco Secure Policy Manager does not automatically generate the security policies required to permit this syslog traffic to traverse Managed Devices. You must manually define and apply any security policies required to enable the traversal of such traffic across a Managed Device. If the target syslog server resides on a network that is directly connected to an interface on the Managed Devices, Cisco Secure Policy Manager does generate the command set that is required to ensure that the syslog data streams are sent to that syslog server.

Tips If you chose to send the syslog data streams to a host that runs a third-party syslog server, you must also define that host in the Network Topology tree and add the syslog client/server product type to that host.

By studying and recording audit records based on syslog data streams, the Policy Monitor Point enables you to generate and view reports about network and device activity, as well as generate e-mail and pager-based notifications about specific activities. However, you are not required to specify that you want a Cisco Secure Policy Manager host to monitor these data streams. You can also specify that you want to distribute these data streams to other hosts that run syslog servers. Many administrators use such syslog servers to study audit records for particular usage patterns, and they often run additional scripts to study network activity and generate usage and departmental billing statistics.

Tips Because syslog data streams use UDP and because of the high volume of data that a Managed Device can generate, we strongly recommend that you locate your Policy Monitor Point on the network directly attached to an inside interface of the Managed Device. For very high volume Managed Devices, we recommend that you dedicate a small DMZ network for monitoring purposes. You can do this using an internal router or switch or by installing an additional interface in the Managed Device and attaching the DMZ network directly to

RQS Nº 03/2005 - CN - CPMI - CORREIOS
1279
Fls:
Doc:

the Managed Device. This configuration prevents you from flooding your networks with UDP packets and offers a more reliable connection for syslog data.

Caution: Using Mapping Rules that Effect Policy Distribution Point Traffic

If you define a static translation rule for a Policy Distribution Point, you can cause a temporary command set publishing problem. The problem results because the connection to the Managed Device is broken once the new command set is published to the Managed Device because it effectively changes the address of the Cisco Secure Policy Manager host by which the current command set is being published.

In this case, you have two possible solutions to resolve this temporary problem:

1. Define a temporary policy that allows the administrative network service from the old Policy Distribution Point address to the administrative network interface in the Managed Devices that use that Policy Distribution Point. You only need to define the policy to allow the old IP address because the policy that allows the new IP address is automatically generated and applied in the Cisco System Folder. After you publish the command sets, remove the temporary policy and regenerate/publish the command sets.
2. Another approach is to use the Prologue option in the Command panel for the affected Managed Devices to specify that you want to accept administrative connections manually from the old IP address. After you publish the command sets, you can remove the line and republish.

Task List for the Control Panel

You can perform the following tasks from the Control panel. For step-by-step procedures on performing a specific task, see the corresponding section.

- "Modifying the IP Address Setting used to Manage the Managed Device" section on page 6-20
- "Selecting the Policy Distribution Point that Manages a Managed Device" section on page 6-22
- "Requiring that a Managed Device Use an IPSec Tunnel for Administration" section on page 6-22
- "Selecting the Policy Monitor Point Associated with a Managed Device" section on page 6-24
- "Selecting the Syslog Servers Associated with a Managed Device" section on page 6-24
- "Specifying the Enable Password used to Administer a Managed Device" section on page 6-25
- "Specifying the Telnet Password used to Administer a Managed Device" section on page 6-26

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1280
Doc: 3701

- "Viewing the Associated Network Service on a Managed Device" section on page 6-27
- "Viewing the TCP Port used by the Managed Device for Administrative Purposes" section on page 6-27

Modifying the IP Address Setting used to Manage the Managed Device

You can specify the IP address that a Cisco Secure Policy Manager host acting as a Policy Distribution Point uses to contact the Managed Device for the purpose of publishing the derived network policies and to obtain status about the Managed Device. This IP address must be an IP address assigned to an interface of the Managed Device. This IP address can also be the IP address used by any other administrative tools that you use to review the status of this Managed Device.

Note For Managed Devices based on 4.x and earlier versions of PIX Firewall software, you cannot assign an IP address that is assigned to the outside interface of a PIX Firewall. The IP address must be assigned to the inside interface or one of the perimeter interfaces.

To modify the IP address used to connect to the Managed Device, follow these steps:

Step 1 Right-click the right-click the **PIX Firewall** icon, **IOS Router** icon, or the **Sensor** icon for which you want to modify the IP address used to distribute command sets to that Managed Device.

Step 2 To view the **Control** panel, point to **Properties** and click **Control** on the shortcut menu.

Result: The Control panel appears in the View pane.

Step 3 To change the IP address on which the Managed Device listens for requests from the Policy Distribution Point and other administrative tools, select the new IP address in the **IP Address** box under **General Settings**.

The list of IP addresses available are those IP addresses that are defined for the valid interfaces of this Managed Device. These addresses are defined in the Interfaces panel of the selected Managed Device node. By default, the Control panel uses the first IP address listed under the first interface attached to an upstream network.

Caution If you modify the IP address that Cisco Secure Policy Manager uses to publish the commands to a Managed Device (the address in the Control panel), you must define an intermediate security policy to allow the network service selected on the Control panel to that enables both the old and the new IP addresses. Otherwise, the connection to the Managed Device is broken while the Policy Distribution Point is publishing the command set that changes from the old address to the new address.

Step 4 To accept your changes and close the selected panel, click **OK**.

Step 5 To save any changes that you have made, click **Save** on the **File** menu.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1281
Doc: 3701

Selecting the Policy Distribution Point that Manages a Managed Device

From the Control panel, you can specify the Policy Distribution Point that is used to publish new network policies to the Managed Device. This Policy Distribution Point is responsible for generating and publishing network policies to Managed Devices, such as the PIX Firewall, IOS router, or IDS sensor.

To select the Policy Distribution Point used to publish network policy to the Managed Device, follow these steps:

Step 1 Right-click the **PIX Firewall** icon, **IOS Router** icon, or the **Sensor** icon for which you want to select the associated Policy Distribution Point.

Step 2 To view the **Control** panel, point to **Properties** and click **Control** on the shortcut menu.

Result: The Control panel appears in the View pane.

Step 3 To select the host that is running the Policy Distribution Point that you want to use, click that host name in the **Policy Distribution Point** box under **Policy Distribution**.

This box displays only those primary and/or secondary servers defined under the Network Topology tree that have a Policy Distribution Point client/server product installed on them.

If you installed a standalone Cisco Secure Policy Manager, the Policy Distribution Point resides on that primary server. Otherwise in a distributed installation, it can reside on either a primary or secondary server, depending on which feature sets you chose to install on the various hosts.

Step 4 To accept your changes and close the selected panel, click **OK**.

Step 5 To save any changes that you have made, click **Save** on the **File** menu.

Requiring that a Managed Device Use an IPSec Tunnel for Administration

From the Control panel, you can specify that you want the Cisco Secure Policy Manager host acting as the Policy Distribution Point to use an IPSec tunnel when communicating with the Managed Device, such as a PIX Firewall or IOS router. This tunnel can provide additional authentication, as well

as encryption, for sessions that occur between the Managed Device and the Policy Distribution Point, providing non-repudiation and data integrity for the network policies that are published to the Managed Device.

To require Cisco Secure Policy Manager to use an IPSec tunnel when communicating with the Managed Device, follow these steps:

Step 1 Right-click the **PIX Firewall** icon, **IOS Router** icon, or the **Sensor** icon for which you want to require the use of an IPSec tunnel.

Step 2 To view the **Control** panel, point to **Properties** and click **Control** on the shortcut menu.

Result: The Control panel appears in the View pane.

Step 3 To select the IPSec Tunnel Template definition used to connect to the selected Managed Device, click that template in the **Use secure IPSec with template** box under **Policy Distribution**.

This template must be defined under the IPSec Tunnel Templates branch of the Tools and Services tree. By default, the Policy Distribution Point does not use an IPSec tunnel when communicating with the Managed Device.

Caution For IDS sensors, you can only select IPSec Tunnel Templates that are based on manual keys. IDS sensors do not support IKE.

Step 4 To accept your changes and close the selected panel, click **OK**.

Step 5 To save any changes that you have made, click **Save** on the **File** menu.

Step 6 Before publishing the command set to the Managed Device, you must first configure the Managed Device to accept the IPSec tunnel from the Policy Distribution Point. To configure the Managed Device, refer to the *IPSec Tunnel Implementation* administrator's guide.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1282
3701
Doc:

Selecting the Policy Monitor Point Associated with a Managed Device

From the Control panel, you can specify the Policy Monitor Point that is used to monitor the syslog data streams generated by the Managed Device, such as a PIX Firewall or IOS router. This Policy Monitor Point studies the syslog data to derive higher-level audit records, such as session records.

To select the Policy Monitor Point used to monitor Managed Device syslog data streams, follow these steps:

Step 1 Right-click the **PIX Firewall** icon or **IOS Router** icon for which you want to select a Policy Monitor Point, point to **Properties**, and click **Control** on the shortcut menu.

Result: The Control panel appears in the View pane.

Step 2 To select the host that is running the Policy Monitor Point that you want to use, click that host name in the **Policy Monitor** box under **Logging**.

This box displays only those primary and/or secondary servers defined under the Network Topology tree that have a Policy Monitor Point client/server product installed on them.

Step 3 To accept your changes and close the selected panel, click **OK**.

Step 4 To save any changes that you have made, click **Save** on the **File** menu.

Selecting the Syslog Servers Associated with a Managed Device

From the Control panel, you can specify one or more syslog servers, in addition to the Cisco Secure Policy Manager host acting as Policy Monitor Point, that you can use to provide additional monitoring of the syslog data streams generated by the Managed Device.

To select the syslog servers used to monitor Managed Device syslog data streams, follow these steps:

Step 1 Right-click the **PIX Firewall** icon or **IOS router** icon for which you want to select an associated syslog server, point to **Properties**, and click **Control** on the shortcut menu.

Result: The Control panel appears in the View pane.

3960
21

Step 2 To select one or more hosts on which syslog servers are running, click those host names in the **Syslog Monitors** box under **Logging**.

This box displays only those hosts defined under the Network Topology tree that have a syslog client/server product installed on them. The host or hosts that you select must have a syslog application capable of processing the data streams. For instructions on installing and configuring these applications, refer to the documentation that came with those products.

Step 3 To accept your changes and close the selected panel, click **OK**.

Step 4 To save any changes that you have made, click **Save** on the **File** menu.

Specifying the Enable Password used to Administer a Managed Device

From the Control panel, you can specify the enable password for the selected Managed Device. The Policy Distribution Point uses this password to authenticate to the Managed Device before it can publish new network policies to that Managed Device.

To specify the enable password used to publish network policies to the Managed Device, follow these steps:

Note All Managed Devices require that you specify the enable password.

Step 1 Right-click the **PIX Firewall** icon, **IOS Router** icon, or the **Sensor** icon for which you want to specify the enable password.

Step 2 To view the **Control** panel, point to **Properties** and click **Control** on the shortcut menu.

Result: The Control panel appears in the View pane.

Step 3 To specify the enable password, type that password in the **Enable password** box under **Authentication**.

The enable password can be up to 16 alphanumeric characters. Also, you can use both uppercase and lowercase characters. This password is case sensitive.

IRQS Nº 03/2005 - CN
CPMI - CORREIOS
1283
Fls:
Doc: 3701

Step 4 To accept your changes and close the selected panel, click **OK**.

Step 5 To save any changes that you have made, click **Save** on the **File** menu.

Specifying the Telnet Password used to Administer a Managed Device

From the Control panel, you can specify the Telnet password for the selected Managed Device. Any administrators who connect to the Managed Device to perform any diagnostic tests must first use this password to authenticate to the Managed Device.

To specify the Telnet password used to authenticate to the Managed Device, follow these steps:

Note Only the IOS router uses (and requires) the Telnet password. However, both the PIX Firewall and the IOS router require that you specify the enable password.

Step 1 Right-click the **PIX Firewall** icon or **IOS Router** icon for which you want to specify the Telnet password.

Step 2 To view the **Control** panel, point to **Properties** and click **Control** on the shortcut menu.

Result: The Control panel appears in the View pane.

Step 3 To specify the Telnet password, type that password in the **Telnet password** box under **Authentication**.

The Telnet password can be up to 16 alphanumeric and special characters; however, you cannot use the question mark, space, or colon in the password. You can use both uppercase and lowercase characters, because this password is case sensitive.

Step 4 To accept your changes and close the selected panel, click **OK**.

Step 5 To save any changes that you have made, click **Save** on the **File** menu.

Viewing the Associated Network Service on a Managed Device

Modifying the network service associated with a Managed Device has no effect on the system or the configuration of that Managed Device. It identifies the network service that Cisco Secure Policy Manager uses to publish the generated command sets to that Managed Device. This network service is also used to return status updates to Cisco Secure Policy Manager about the publishing status.

For an IOS router, this network service is Telnet on (TCP port 23). For a PIX Firewall, this network service is PIX Secure Telnet (TCP 1467). For an IDS sensor, this network service is postoffice (UDP 45000).

Viewing the TCP Port used by the Managed Device for Administrative Purposes

Modifying the port used for the network service associated with a Managed Device has no effect on the system or the configuration of that Managed Device. For an IOS router, this network service is Telnet on (TCP port 23). For a PIX Firewall, this network service is PIX Secure Telnet (TCP 1467). For an IDS sensor, this network service is postoffice (UDP 45000).

IPSec Panel

The IPSec panel appears on a node that has the IPSec Support option enabled on its General panel. The node can be a gateway object or a Cisco Secure Policy Manager host. From the IPSec panel, you can specify the device-specific settings that are used to support different types of IPSec tunnel templates.These settings include the type of DES cipher that this node supports. In addition, you can specify the device-specific settings required to support an IKE authentication scheme when establishing an IPSec session with a valid peer.You must specify these settings if this node is included in an IPSec tunnel group definition that is based on a template that uses IKE as the authentication mechanism. These settings include the type of shared secret and the secret's value. You must specify these device-specific settings for each IKE authentication scheme identified by the templates used in the IPSec tunnel group definitions that identify this node as a peer.

IRQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1284
Doc: 3701

Learn More About IPSec Support on Network Objects

You must enable IPSec support on all IPSec peers before you establish IPSec tunnel groups that consist of those peers. A PIX Firewall, IOS router, Cloud, generic Router, or Cisco Secure Policy Manager host can act as an IPSec peer. Specifying the settings in the IPSec panel for a IPSec-enabled node prepares that node to serve as an endpoint, or peer, in an IPSec tunnel group.

When you want to define a *control channel* tunnel group, which uses IPSec tunnels to communicate between the Policy Distribution Point and a specific Managed Device that supports IPSec, you must bootstrap each IPSec-enabled Managed Device to ensure that it can act as a peer in that IPSec tunnel group definition. While you have to bootstrap the Managed Devices, you do not have to bootstrap the Cisco Secure Policy Manager hosts.

When a Cisco Secure Policy Manager host participates in an IPSec tunnel group, it is used to securely publish generated commands sets to a Managed Device, such as a PIX Firewall or IOS router. However, for a Cisco Secure Policy Manager host to act as an IPSec peer, you must have the Cisco Secure VPN Client software installed and operational on the host that is acting as the Policy Distribution Point that will be participating in the IPSec tunnel.

If this node is not a Cisco Secure Policy Manager host, it must be a gateway object that is capable of participating in an IPSec tunnel. As an IPSec-capable gateway object, the node can participate in two types of tunnels:

- If the gateway object is a Managed Device, it can participate in an IPSec tunnel between the Cisco Secure Policy Manager host that is responsible for generating and publishing the device-specific command sets to that Managed Device.
- Whether the gateway object is managed or not, it can participate in a tunnel between itself and another gateway object, which acts as a peer for a specific IPSec session.

From the IPSec panel associated with a node, you can specify three types of settings related to the use of IPSec by this node:

- The strongest DES cipher that this node can support when encrypting the ESP payload and for encrypting the AH packets
- The use of a certificate authority server by this node
- The details of the pre-shared keys used by this node on a per-peer basis

In addition, you can discover the properties of the certificate currently installed on this node, if you have chosen to use certificates and have previously loaded the certificate on this node during the bootstrap process.

Specifying the DES Cipher

The DES cipher setting allows you to specify the strongest cipher that this node supports for encryption of IPSec session packets. If this node type can support triple DES, you should select that cipher for this value. Because Cisco IPSec products support only DES, and not all version support triple DES, these two ciphers are the only valid ciphers within Cisco Secure Policy Manager.

When you specify triple DES as the strongest cipher, this value does not mean that triple DES will be used by all IPSec Tunnel Groups in which this node is defined as a peer. If the other peers do not support triple DES, this node can still be used with IPSec Tunnel Templates that specify standard DES as the cipher. Cisco Secure Policy Manager uses this DES cipher setting to perform a consistency check to verify that your IPSec Tunnel Group definitions are based on IPSec Tunnel Templates that the peers in the group can support.

For additional information on encryption, ciphers, and how encryption works, refer to the *Cisco Secure Policy Manager Administrator's Guide: IPSec Tunnel Implementation*.

Enabling Certificate Authority Support

If you specify that you want this node to use a certificate authority server for the purpose of refreshing the certificates, Cisco Secure Policy Manager automatically creates and applies a security policy that enables HTTP traffic to pass between this node and the specified certificate authority server. Before you can select a certificate authority server, you must first define that server under the Network Topology tree.

Certificate authority servers use HTTP as the protocol for renewing and validating certificates. They manage data about when the certificates managed by the server expire and the rules for automatically refreshing or issuing new certificates to the network objects that are subscribers to that certificate authority. In addition, certificate authority servers provide support for certificate revocation lists (CRLs), which enable you to specify that certain certificates should not be trusted.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1285
Fls:
Doc: 3701

If at some point the selected network object no longer requires access to this certificate authority server, you must clear the selection in the Trusted Certificate Authority box in the IPSec panel.

Specifying the Type of Secret to Use with IKE

IKE is a protocol that negotiates the parameters required to set up an IPSec tunnel. This negotiation protocol is used to determine the common DES cipher and establish the initial secret keys for the session. In the IPSec panel, you can define the settings for two types of IKE negotiations:

- Negotiations based on a pre-shared secret
- Negotiations based on a certificate

Pre-shared keys offer a simple, yet secure, solution for smaller networks because they do not require the support of a public key infrastructure (PKI). Pre-shared keys enable you to define a common shared secret to be used by two peers that are capable of using IKE to negotiate the settings for a specific IPSec session. Because IKE periodically negotiates new session keys for use when encrypting the network packets of an IPSec session during that session, pre-shared secrets offer a more secure IPSec solution than manual keys, which generate only one pair of session keys. In addition, because pre-shared keys enable you to specify a single secret that is shared between each peer pair, the key administration is also simpler than that of IPSec solutions based on manual keys.

To overcome the day-to-day key administration issues involved in changing pre-shared keys in accordance with a strong organizational security policy, you can also specify that you want an IPSec-enabled network object to use a digital certificate (sometimes referred to as RSA certificate signatures) as the shared secret that peers use to authenticate that network object. In this configuration, the IPSec-enabled network object publishes its public key to its peers, which use that certificate to authenticate that network object.

Unlike pre-shared keys, certificates enable IPSec peers to authenticate using a trusted certificate authority. Because they do not require an IPSec-enabled network object to know a pre-shared secret for each of its peers, digital certificates are more scalable, which means they can support larger enterprise networks. While digital certificates are more technologically complex than pre-shared keys and they require the support of a PKI within your organization (including the purchase of a certificate from a trusted certification authority), they also offer a

more secure method of authentication because the certificates can be configured to expire at which time new certificates can be issued automatically by a certificate authority server.

Discovering Certificate Information

If you have previously configured this node to use a certificate when performing IKE negotiations, you can discover the properties of that certificate by clicking Discover.

This discovery process queries the node about that certificate and retrieves information, such as who issued the certificate, the serial number of the certificate, and the dates for which the certificate is valid.

You can use this information to ensure that you have the proper certificate loaded and to stay abreast of possible problems, such as expiration.

Task List for the IPSec Panel

You can perform the following tasks from the IPSec panel on an IPSec-enabled gateway object, such as a PIX Firewall, IOS router, generic Router, or Cloud, that is defined within the Network Topology tree. In addition, if you have installed Cisco Secure VPN Client software on a Policy Distribution Point that published command sets to a Managed Device, you can perform these tasks from the IPSec panel associated with the Cisco Secure Policy Manager host that acts as that Policy Distribution Point. For step-by-step procedures on performing a specific task, see the corresponding section.

- "Specifying DES Cipher Settings on the IPSec Panel" section on page 6-32
- "Specifying Pre-Shared Secrets for IKE" section on page 6-32
- "Configuring a Certificate" section on page 6-34
- "Discovering Certificate Information" section on page 6-35

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1286
Doc: 3701

Specifying DES Cipher Settings on the IPSec Panel

From the IPSec panel, you can identify the strongest DES cipher that the selected node supports. Cisco Secure Policy Manager uses this information to perform consistency checks that validate that all peers in IPSec Tunnel Group definitions based on IPSec Tunnel Templates that require specific ciphers can support those ciphers.

To specify the strongest DES cipher that this node can support, follow these steps:

Step 1 Right-click the gateway object icon that has IPSec Support enabled in its General panel for which you want to specify the DES cipher support settings, point to **Properties** and click **IPSec** on the shortcut menu.

Result: The IPsec panel appears in the View pane.

Step 2 To specify which DES cipher is supported by this node, click that cipher in the list of ciphers in the **DES Cipher Support** box.

Two types of DES ciphers are available, depending on the type of software that is running on the selected node:

- **DES**—This option identifies that the node can support the standard DES cipher for IPsec-based communications, including the IKE authentication and the ESP payloads. If DES is not supported by the peer, the IPSec session request fails. All peers must, at a minimum, support the standard DES cipher.
- **triple DES**—This option identifies that the node can support the triple DES cipher. If a peer does not support triple DES, a node that supports triple DES can also support the standard DES cipher for the duration of a session.

Step 3 To accept your changes and close the selected panel, click **OK**.

Step 4 To save any changes that you have made, click **Save** on the **File** menu.

Specifying Pre-Shared Secrets for IKE

From the IPSec panel, you can specify a pre-shared secret that is used to perform IKE negotiations between the selected node and its IPSec tunnel group peers. Cisco Secure Policy Manager uses this secret to generate the device-specific commands that enable these pre-shared secrets on this node and its peers. You

only need to specify this secret in this panel, as it is propagated to the IPSec panels for the specified peers. In other words, you only have to specify a shared secret on one of the two peer nodes.

To specify the secrets to share between this node and its peers, follow these steps:

Step 1 Right-click the gateway object icon that has IPSec Support enabled in its General panel for which you want to specify the pre-shared keys to use with peers when negotiating the IPSec sessions based on IKE, point to **Properties** and click **IPSec** on the shortcut menu.

Result: The IPsec panel appears in the View pane.

Step 2 To specify the peer for which you want to define a pre-shared secret between the selected node and that peer, click that peer in the list of available peers in the **Tunnel Peers** box.

Result: The Secret shared with peer label displays the name of the selected peer.

This list contains only those gateway objects and Cisco Secure Policy Manager hosts defined under the Network Topology tree that have the IPSec Support option selected in the General panel.

Step 3 To specify the secret to share between this node and the peer selected in the **Tunnel Peers** box, type that secret in the **Secret shared with peer** box.

This secret identifies a valid secret that can be used by IKE to set up an IPSec tunnel between this node and the selected peer. The minimum length for this secret value is 8 characters and the maximum length is up to 128 alphanumeric characters. You cannot use Tab, Enter, spaces, question marks, or double quotes when defining this shared secret.

Step 4 For each peer that you want to define a pre-shared secret, repeat Steps 5 and 6.

Step 5 To accept your changes and close the selected panel, click **OK**.

Step 6 To save any changes that you have made, click **Save** on the **File** menu.

To generate a new command set that includes the pre-shared secrets required by each peer, you must perform a Save and Update operation.

ROS Nº 03/2005 - CN
CPMI - CORREIOS
1287
Fls:
3701
Doc:

Configuring a Certificate

From the IPSec panel, you can identify that you want the selected node to be able to communicate with a certificate authority server that is defined under the Network Topology tree. Certificate authority servers use HTTP as the protocol for renewing and validating certificates. They manage data about when the certificates managed by the server expire and the rules for automatically refreshing or issuing new certificates to the network objects that are subscribers to that certificate authority. In addition, certificate authority servers provide support for certificate revocation lists (CRLs), which enable you to specify that certain certificates should not be trusted.

Tips Cisco Secure Policy Manager creates and applies a security policy that permits HTTP traffic to pass between this node and the specified certificate authority server.

To specify the certificate authority server to use for this node, follow these steps:

Step 1 Right-click the gateway object icon that has IPSec Support enabled in its General panel, point to **Properties** and click **IPSec** on the shortcut menu.

Result: The IPsec panel appears in the View pane.

Step 2 To specify which certificate authority server to use with this node, click that server in the list of certificate authority servers in the **Trusted Certificate Authority Server** box.

This value identifies a host defined in the Network Topology tree that has been configured to identify a certificate authority server by adding the Certificate Authority client-server product type to that host.

Step 3 To accept your changes and close the selected panel, click **OK**.

Step 4 To save any changes that you have made, click **Save** on the **File** menu.

Discovering Certificate Information

From the IPSec panel, you can discover specific information about any certificates that are installed on a Managed Device that has the IPSec Support option selected in the General panel for that Managed Device node.

To discover the certificate information, follow these steps:

Step 1 Right-click the **PIX Firewall** icon or **IOS Router** icon that has IPSec Support enabled in its General panel and has a previously configured certificate installed on that Managed Device for which you want to discover the certificate information, point to **Properties** and click **IPSec** on the shortcut menu.

Result: The IPsec panel appears in the View pane.

Step 2 To specify that you want to discover the information about the certificates used by this node, click **Discover**.

Result: The Discovery dialog box appears with the IPSec box selected under the Discovery Selections box.

Step 3 To discover the certificate information and other IPSec settings for this node, click **Discover**.

Result: The Discovery Status box displays the status of the device discovery, including the time remaining before the discovery process aborts its discover attempt. When this process is complete, a message stating "Configuration completed. The configuration attempt was successful" appears. In addition, the Results button appears, which when clicked provides information about the discovery in the Discovery Results dialog box. Specifically, the Discovery Results dialog box should display the following messages:

- IPSec capability detected.
- Triple DES capability detected. (This message only appears if this node supports triple DES.)
- # certificates detected. (Where # is the number of certificates discovered on this node.)

Step 4 To close the **Discovery** dialog box, click **OK**.

Result: The IPSec panel now displays information about each certificate that was discovered. This information is organized on separate subtabs (below the Trusted Certificate Authority box) for each certificate that is discovered.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1288
Fls:
Doc: 3701

Step 5 To accept your changes and close the selected panel, click **OK**.

Step 6 To save any changes that you have made, click **Save** on the **File** menu.

AAA

AAA (authentication, authorization, and accounting) uses TACACS+ and RADIUS protocols to seamlessly integrate security features.

Cisco Secure Policy Manager implements AAA to enforce authentication, accounting, and authorization for pass-through and administrative traffic. Pass-through traffic passes from a source through a Managed Device to a destination. Administrative traffic passes from the Cisco Secure Policy Manager host to the Managed Device.

Learn More About AAA

This topic provides an overview of AAA (authentication, authorization, and accounting) and how Cisco Secure Policy Manager uses the TACACS+ and RADIUS protocols to implement AAA. For more information about the AAA architecture, see RFC2904 and RFC2989.

- *Authentication* identifies users before they are permitted access to the network or network services. Authentication provides the method for identifying users, including login and password dialog, challenge and response, messaging support, and depending on the security protocol selected, encryption.
- *Authorization* assembles a set of attribute-value pairs that describe privileges for the identified user. These attribute-value pairs are compared to the information contained in a TACACS+ or RADIUS server database.
- *Accounting* logs the services accessed and the network resources consumed by users. Accounting provides the method for collecting and distributing information such as user identities, start and stop times, executed commands, number of packets, and number of bytes.

Implementing and managing a AAA-based security solution is complicated by the number of network elements and the complexity of the device configuration. However, Cisco Secure Policy Manager integrates AAA to replace tedious device-level configurations with simple, intuitive, high-level AAA security policies. After Cisco Secure Policy Manager is configured to permit AAA, all necessary per-device configurations are generated automatically.

In the Cisco Secure Policy Manager implementation of AAA, you can enforce authentication, accounting, and authorization for pass-through traffic or administrative traffic. Pass-through traffic passes through a Managed Device from a source to a destination. Administrative traffic passes from the Cisco Secure Policy Manager host to the Managed Device. See the following checklists for more information about configuring Cisco Secure Policy Manager to authenticate pass-through and administrative traffic.

- Checklist for Authenticating Pass-Through Traffic, page 6-39. Provides information for configuring Cisco Secure Policy Manager to authenticate pass-through traffic.
- Checklist for Authenticating Administrative Traffic, page 6-37. Provides information for configuring Cisco Secure Policy Manager to authenticate administrative traffic.

Cisco Secure Policy Manager uses AAA servers and authentication proxies (both in the **Network Topology** tree) and policy to support AAA. The AAA server is a host in your topology and runs either TACACS+ or RADIUS services. The authentication proxy is the gateway device that communicates between a client requesting AAA services and the AAA server. Finally, Cisco Secure Policy Manager uses security policies to define which traffic should be authenticated.

Checklist for Authenticating Administrative Traffic

You can specify that a AAA server authenticate administrative traffic between a Policy Distribution Point and the Managed Device that it controls. Using authentication information presented by the Policy Distribution Point, the Managed Device queries the TACACS+ server. A Managed Device will query the TACACS+ servers, in the order they were specified, until an active server is found. If no active server or match for the username is found, the session request is rejected.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1289
Doc: 3701

Note Only TACACS+ servers can authenticate administrative traffic for a Managed Device.

The following checklist outlines the steps required to authenticate administrative traffic. Each step may contain several substeps and should be performed in the order presented. References to the specific tasks for each step are provided as well.

Step 1 Set Up the AAA Server

If you want to authenticate administrative traffic, you must create a AAA server in your network topology with the appropriate services. Then, you can configure the Managed Devices to accept authenticated administrative traffic. This involves performing the following tasks:

1. Adding the AAA server host to the **Network Topology** tree (if it does not appear in the tree).
2. Adding the TACACS+ service to the AAA server host in the **Network Topology** tree.

For more information, see the following references:

1. Creating a Host Node, page 4-67
2. Authentication Server Panel, page 4-70

Step 2 Configure the Managed Device

For each Managed Device that will receive authenticated administrative traffic, specify the AAA server(s) that will authenticate the administrative traffic. Then, manually enter the AAA bootstrap commands.

For more information, see the "AAA" section on page 6-36.

Step 3 Generate the Command Sets

The command sets are automatically generated when you save and update your Cisco Secure Policy Manager configuration.

If Cisco Secure Policy Manager automatically publishes the command sets to the Managed Devices when you click **Save and Update** on the **File** menu, you must disable this feature before generating the command sets.

For more information, see the Cisco *Secure Policy Manager Administrator's Guide: Policy Development and Enforcement*.

Step 4 Publish the Commands to the Managed Device

Publishing the command sets to the Managed Device is a two-step process.

First, you have to bootstrap each Managed Device manually. Because you have configured Cisco Secure Policy Manager to communicate with the Managed Device through authenticated traffic, Cisco Secure Policy Manager will immediately try to do so. However, the Managed Device has not been configured to accept the authenticated traffic. The first step enables the Managed Device to accept the authenticated traffic.

Then, you must publish the command sets to the Managed Device.

We recommend that you perform the following two steps for each Managed Device. Start with the most remote Managed Device and work your way to the closest. In this case, *remote* refers to a Managed Device that is located behind another Managed Device from the point of view of the Policy Distribution Point.

1. Bootstrap the Managed Device.
2. Publish the command set to the Managed Device.

Repeat Step 1 and Step 2 for each Managed Device that will accept authenticated administrative traffic from Cisco Secure Policy Manager.

For more information, see the *Policy Development and Enforcement* administrator's guide.

Checklist for Authenticating Pass-Through Traffic

You can specify that a AAA server authenticate traffic passing through a Managed Device. In this implementation of AAA, a *client* is the source in a security policy abstract that is requesting services through an authentication proxy. An *authentication proxy* is the gateway device that communicates between a client and the AAA server. The *AAA server* is the host that provides TACACS+ or RADIUS services (authentication, authorization, and accounting). The AAA server provides these services as specified by the security policy abstract that contains a Use Authentication node.

The following checklist outlines the steps required to authenticate pass-through traffic. Each step may contain several substeps and should be performed in the order presented. References to the specific tasks for each step are provided as well.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1290
Doc: 3701

Step 1 Set Up the AAA Server

If you want to authenticate pass-through traffic, first you must create a AAA server in your network topology with the appropriate services. Then, you can configure the Managed Devices to accept authenticated administrative traffic. This involves performing the following tasks:

1. Adding the AAA server host to the **Network Topology** tree (if it does not appear in the tree).
2. Adding the TACACS+ or RADIUS service to the AAA server host in the **Network Topology** tree.

For more information, see the following references:

1. Creating a Host Node, page 4-67
2. Authentication Server Panel, page 4-70

Step 2 Configure the Managed Device

You must specify the AAA server(s) that will authenticate pass-through traffic for each Managed Device that will serve as an authentication proxy. Then, manually enter the AAA bootstrap commands.

For more information, see the "AAA" section on page 6-36.

Step 3 Create Policy

Although you have defined the AAA server(s) and AAA parameters for each Managed Device, you have not yet defined the services that will require authentication. The final steps in the process are to create policies that require authentication for selected services, generate the device-specific command sets for those policies, and publish the command sets to the Managed Devices.

For more information, see the *Cisco Secure Policy Manager Administrator's Guide: Policy Development and Enforcement.*

Learn More About the AAA Panel

In Cisco Secure Policy Manager, AAA support (authentication, authorization, and accounting) refers to Managed Devices that use authentication servers (AAA servers), either TACACS+ (see the "Learn More About TACACS+ Authentication Servers" section on page 4-72) or RADIUS (see the "Learn More About RADIUS

Authentication Servers" section on page 4-71), to authenticate users on your network. While Cisco Secure Policy Manager does not manage the services provided by AAA servers (the AAA applications manage those services and the user database), you need to be able to distinguish among the services:

- *Authentication* requires a requesting user to provide a username and password pair that is used to validate that user's identity.
- *Authorization* enables privileges for a requesting user based on profiles that define specific privileges. These profiles and privileges are stored in the AAA server database.

Note The Cisco Secure PIX Firewall does not authorize when using RADIUS.

- *Accounting* logs service requests, providing user-based audit trails.

Users are authenticated against usernames and group profiles stored on the AAA server. Managed Devices are network devices that initiate an authentication request to the AAA server whenever a network service request traverses a Managed Device.

An authentication attempt is denied for one of three reasons: the username is not found in the AAA server database, the requesting user provides the incorrect username/password pair, or the AAA server is unreachable by the Managed Device.

A Cisco Secure PIX Firewall only considers the first AAA server in the list for either type of authentication. In other words, defining multiple servers for a Cisco Secure PIX Firewall has no effect. If for any reason the authentication attempt fails or times out to that first server, the Cisco Secure PIX Firewall rejects that session request.

However, the Cisco router running Cisco Secure Integrated Software and the router running Cisco IOS software both allow authentication attempts to time out. In this case, the AAA server is assumed to be unavailable or down. If the authentication attempt times out, the Cisco router running Cisco Secure Integrated Software or the router running Cisco IOS software contacts the next server in the list. If the username is not found in the AAA server database, the session request is denied.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1291
Doc 3701

Note Before you can enable a Managed Device to use a AAA server, you must create a Host node in the Network Topology tree and add either a TACACS+ or RADIUS client/server product type to that host. In addition, you must bootstrap the Managed Device so that the Policy Distribution Point host can authenticate to and administer it.

In addition, Cisco Secure Policy Manager can use AAA servers to authenticate to a Managed Device when publishing commands to that Managed Device. If you want a Managed Device to authenticate such administrative traffic, use the Control panel of each Managed Device to define the AAA username and password that the Policy Distribution Point should use to authenticate to the TACACS+ server.

Note To use AAA to authenticate IPSec-based traffic flows, you must enable **xauth** in the General panel of the IPSec tunnel template for IPSec tunnel groups.

Virtual Addresses and Cisco Secure PIX Firewall

Cisco Secure PIX Firewall uses virtual addresses during authentication of pass-through traffic. If you use a Cisco Secure PIX Firewall as an authentication proxy, select HTTP, FTP, or Telnet as the protocol that a client should use to initiate AAA services. If you select HTTP or Telnet, Cisco Secure PIX Firewall uses a virtual HTTP or Telnet server to intercept the HTTP or Telnet request during pre-authentication communications with the client and the AAA server.

Cisco Secure Policy Manager generates the necessary commands to permit the authentication traffic between the client and the authentication proxy; however, you must specify a virtual address for the virtual server on the Cisco Secure PIX Firewall.

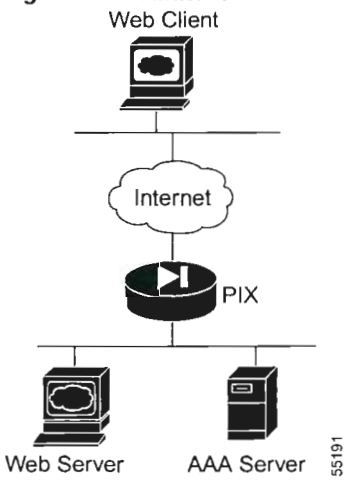
The virtual address identifies the IP address of the virtual HTTP or Telnet server on the Cisco Secure PIX Firewall. The virtual address is any valid, unused IP address that can be routed to the interface of the Cisco Secure PIX Firewall closest to the requesting client. A virtual HTTP server pre-authenticates a user who is requesting HTTP services. A virtual Telnet server pre-authenticates a user who is requesting Telnet services.

Pre-authentication prevents a request from being prematurely denied. In the following example, the Web Server requires a user to log in before browsing the contents. When the user attempts to browse the address in question, an HTTP request is sent from the client (user's computer). The Cisco Secure PIX Firewall requests a AAA user name and password. The user provides the user name and password, which is sent to the AAA server for authentication. However, because the user name and password are sent as part of the HTTP traffic, they are also sent to the Web Server. If the AAA user name and password do not match the user name and password required to log in to the Web Server, the request fails. The virtual HTTP server solves this problem by intercepting the HTTP traffic for pre-authentication before it can be denied.

Figure 6-5 and the following discussion illustrate how Cisco Secure PIX Firewall uses a virtual HTTP or Telnet server to pre-authenticate a user.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1292
Fls:
3701
Doc:

Figure 6-5 Authentication of Pass-Through Traffic using a Virtual HTTP Server



For this scenario, the Cisco Secure PIX Firewall has a basic HTTP server built into its framework. This *virtual* server intercepts HTTP requests from any client specified as the source in a security policy with HTTP as the service and Use Authentication as the non-terminal action.A typical sequence of events follows:

1. User browses to Web Server (virtual IP address). The Web Server initiates authentication for pass-through traffic.
2. The virtual HTTP server on the Cisco Secure PIX Firewall intercepts the connection and splits the request into two parts: the AAA request (user name and password) and the HTTP request (address for Web Server).
3. The virtual HTTP server forwards the AAA request to the AAA server. Assuming the user name and password are correct, the AAA server tells the Cisco Secure PIX Firewall to permit the pass-through traffic.
4. The virtual HTTP server sends the HTTP request to the Web Server.
5. The Web Server receives the request for a page, and, knowing that the request requires authentication, sends the authentication request to the client.
6. The user provides the username and password and, assuming it is the correct one for the server, browses like normal.

Note The same concept applies to virtual Telnet servers.

Keep in mind, you should use caution when selecting a virtual address for the virtual HTTP or virtual Telnet server. If a security policy uses the same address as the virtual address and that address is on a less secure side than the destination, you must create a NAT rule to permit the traffic to the Cisco Secure PIX Firewall.

For example, in Figure 6-6, assume that you want the internal server (10.10.10.30) to be known as 30.30.30.30 to the outside world. Cisco Secure Policy Manager will create the virtual HTTP 30.30.30.30 command, but it does not create a static mapping rule to map the internal host to the virtual IP address. The traffic from the Web Server to the Cisco Secure PIX Firewall will not be routed correctly unless you create the following static mapping rule to map the address of the Web Server to the virtual HTTP address:

Figure 6-6 Static Mapping Rule for Virtual Address

Rule	Translate object	via interface(s)	using address	through	with	mask
50	Web Server	outside	30 .30 .30 .30	30 .30 .30 .30		32

55190

Task List for AAA Panel

You can perform the following tasks from the AAA panel on a Managed Device.For step-by-step procedures on performing a specific task, see the corresponding section.

- "Authenticating Pass-Through Traffic Using a AAA Server" section on page 6-47
- "Authenticating Administrative Traffic Using a AAA Server" section on page 6-45

Authenticating Administrative Traffic Using a AAA Server

You can specify that you want a AAA server to authenticate any administrative traffic between a Policy Distribution Point and the Managed Device it controls. Using authentication information presented by the Policy Distribution Point, the

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1293
Doc: 3791

Managed Device queries each TACACS+ server. These TACACS+ servers are queried in order, from top to bottom, until an active server is detected or the list of servers is exhausted. If no match is found, the session request is rejected.

Note Only TACACS+ servers can authenticate administrative traffic for a Managed Device.

To specify which AAA servers should authenticate the administrative traffic used to control the Managed Device, follow these steps:

Step 1 Right-click the **gateway object** icon on which you want to specify the TACACS+ servers to use for authenticating administrative traffic, point to **Properties**, and then click **AAA** on the shortcut menu.

Result: The AAA panel appears in the View pane.

Step 2 To specify the TACACS+ server that you want to use to authenticate administrative traffic, select that server in the **Available AAA Servers** box and click the **Add** button that corresponds to the **AAA servers for device administration** box.

Note You must specify a AAA username and password pair in the **Control** panel of the selected Managed Device. This information is used to authenticate the Policy Distribution Point to the TACACS+ server.

Result: The TACACS+ server appears in the AAA servers for device administration box.

Step 3 To activate the **AAA key for '***hostname***'** box, select the server that you just added in the **AAA servers for device administration** box.

Step 4 To specify the shared secret to be used between the selected Managed Device and the selected AAA server, type that key in the **AAA key for '***hostname***'** box.

This value must contain at least eight alphanumeric character; however, it cannot include ?, ", a tab character, or a carriage return character (the **Enter** key).

Step 5 For each TACACS+ server that you want to add to the **AAA servers for device administration** box, repeat Steps 2 through 4.

Clicking Move Up and Move Down, you can order the servers in the list. Top-down order determines query order.

Step 6 To accept your changes and close the selected panel, click **OK**.

Step 7 To save any changes that you have made, click **Save** on the **File** menu.

Authenticating Pass-Through Traffic Using a AAA Server

You can specify one or more AAA servers defined in the Network Topology tree that you want the selected Managed Device to use to authenticate traffic that passes through it. The Managed Device queries each AAA server using authentication information presented by the requesting user. These AAA servers are queried in order until an active server is detected or the list of servers is exhausted. If no match is found, the session request is rejected.

To specify which AAA servers should be used to authenticate traffic that traverses a Managed Device, follow these steps:

Step 1 Right-click the gateway object icon on which you want to specify the AAA servers to use for authenticating pass-through traffic, point to **Properties**, and then click **AAA** on the shortcut menu.

Result: The AAA panel appears in the View pane.

Step 2 To specify the server that you want to use to authenticate pass-through traffic, select that server in the **Available AAA Servers** box and click the **Add** button that corresponds to the **AAA servers for pass-through traffic** box.

Result: The AAA server appears in the AAA servers for pass-through traffic box.

Step 3 To activate the **AAA key for '***hostname***'** box, select the server that you just added in the **AAA servers for pass-through traffic** box.

Step 4 To specify the shared secret to be used between the selected Managed Device and the selected AAA server, type that key in the **AAA key for '***hostname***'** box.

This value must contain at least eight alphanumeric character; however, it cannot include ?, ", a tab character, or a carriage return character (the **Enter** key).

Step 5 For each AAA server that you want to add to the **AAA servers for pass-through traffic** box, repeat Steps 2 through 4.

Clicking Move Up and Move Down, you can order the servers in the list. Top-down order determines query order.

Step 6 To accept your changes and close the selected panel, click **OK**.

Step 7 To save any changes that you have made, click **Save** on the **File** menu.

~~RQS Nº 03/2005 - CN -~~
CPMI - CORREIOS
1295
Fls:
Doc:
3701

Security Monitor Overview

Monitoring Center for Security (Security Monitor) is part of the CiscoWorks family of applications. It runs on a CiscoWorks Server and provides a web-based interface for monitoring a variety of Cisco security devices. Additionally, Security Monitor provides the following features:

- A real-time event viewer
- Event notification
- Event reporting
- Event correlation

Version 1.1 of Security Monitor introduces several new features and supports Cisco Intrusion Detection System Sensors running Cisco Intrusion Detection System software version 4.0.

Web-Based Interface

Security Monitor provides a web-based interface, which allows remote access to the application. When accessing the CiscoWorks Server over an unsecure network, you can use CiscoWorks Server SSL connectivity to secure the session. Refer to the CiscoWorks Common Services documentation for more information about using SSL to connect to the CiscoWorks Server.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1-1
Fls: 1296
Doc: 3701

Supported Devices and Monitored Events

You can monitor security events from the following Cisco devices:

Note The Message Format column describes the protocol used to send event data to Security Monitor.

Device	Monitored Events	Message Format
Cisco Intrusion Detection System Sensor	IDS events	• postoffice (Cisco Intrusion Detectio n System software version 3.x and earlier) • RDEP (Cisco Intrusion Detection System software version 4.0 and later)
Cisco IDS Host Sensor	IDS events	Syslog
Cisco IOS router with: • IOS Firewall • Cisco Intrusion • Detection System software	IDS subsystem events	Syslog or postoffice (syslog recommended)
PIX Firewall	All firewall and IDS events	Syslog

Real-Time Event Viewer

Security Monitor Event Viewer provides a near real-time view of security events as they occur on your network. Near real-time refers to the slight delay that may occur as events are detected by your network devices and then propagated to your Security Monitor server. In most cases, this delay is negligible.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
78-15616-01
Fls: 1297
Doc 3701

E C T
1393
CPV

Event Viewer provides a tabular view of the incoming event data. The data is arranged in a hierarchal tree that allows you to drill down quickly to isolate problems and find trends in the event data. You can sort the view based on the various elements of the data, such as signature name. The ability to drill down and reorder the data provides a basic means to perform real-time event correlation.

Event Viewer also provides access to tools that provide additional security information. You can select groups of events to display as a graph. You can resolve IP addresses within events to hostnames. You can launch the Network Security Database to provide details about a signature. And, for some events, you can display "context" data, such as the traffic that actually triggered the event.

Event Notification

Using Event Rules, you can configure Security Monitor to send e-mail notifications when specific criteria are met. You can also use Event Rules to trigger custom scripts. Security Monitor does not support pager notifications directly; however, you can use pager notifications if you have an e-mail gateway to your paging system.

You can use Event Rules to create simple rules that provide notifications when a single event occurs. However, you gain their main benefit by using logical operators to create complex rules. These operators allow you to correlate the events or conditions that trigger the notification. You can also set thresholds that allow you to specify the number of times the criteria must be met before the notification is triggered. Using thresholds allows you to distinguish between purposeful events and random occurrences.

Event Reporting

Event reporting provides a snapshot view of security events on your network. Report filters, such as dates and event type, allow you to refine the information shown in the report. You can run reports on-demand or schedule them to be run regularly. By default, reports are stored in the database. However, you can export the report to an HTML file or send the report to one or more recipients through e-mail.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1-3
Fls: 1298
Doc:
3701

Event Correlation

Security Monitor supports basic event correlation through the Event Viewer, Event Rule, and Reporting subsystems.

When you start the Security Monitor Event Viewer with the setting to view "All IDS Alarms", you see the IDS alarms from all monitored devices. Reordering the columns in the Event Viewer provides you with a flexible view of event data, and multiple ways to correlate those events. You can then reorder the columns in the Event Viewer to correlate the events by specific attributes, such as source address, signature name, and so on. For example, by grouping the events in the Event Viewer by source address, signature name, and then by device, you can determine which devices detected a specific event from a specific source.

In the same manner, you can filter the reports to provide you with a correlated, snapshot view of your event data. Filter options include source and destination addresses of the events, device detecting the event, signature the event matched, and so on. These reports can be scheduled or produced on-demand, and can include information from all the monitored devices. They can also be run for a specific range of dates to provide a historical view of the data.

Event Rules provide an even more flexible manner of event correlation by allowing you to create logical relationships between the IDS events produced by all monitored devices, and then to send e-mail notifications or run a custom script based on the relationships that you define.

Note Security Monitor does not provide correlation of non-IDS syslog events with IDS events using Event Rules.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
78-15616-01
Fls: 1299
Doc:
3701

New Features in Security Monitor 1.1

The following new features have been added to Security Monitor 1.1:

- Support for Cisco Intrusion Detection System software version 4.0. Cisco Intrusion Detection System software version 4.0 uses RDEP (Remote Data Exchange Protocol), a proprietary HTTP-based protocol, instead of the postoffice protocol.
- The ability to import Cisco Intrusion Detection System Sensor communication settings from a remote Management Center for IDS Sensors (IDS MC) server.
- The ability to graph event viewer data.
- The ability to use view statistics about the subcomponents of sensors running Cisco Intrusion Detection System software version 4.0.

ROS Nº 03/2005 - CN
CPMI - CORREIOS
78-15616-01
Fls: 1301
Doc: 3701

DOC
000233

CPL/AC

PREGÃO
050/2003

LOCAÇÃO DE EQUIPAMENTOS DE INFORMÁTICA INCLUINDO ASSISTÊNCIA TÉCNICA E TREINAMENTO

HP INVENT – MANUAL APÊNDICES CX A DS

2003
PASTA 08

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1302
Doc: 3701

Apêndice CXX

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1303
Fls:
3701
Doc:

Defining and Viewing Reports

You can access the reporting features that are available in Monitoring Center for Security (Security Monitor) from the Reports tab. You can generate and view reports about network activities monitored by sensors on your network. The reports include summary reports about alarms, sources, destinations, or a specific sensor on your network. By default, all events monitored by a sensor are retained by Security Monitor. Therefore, unless you delete events from the database, you can generate reports based on all recorded activities.

If the desired event is not being generated, verify that the sensor signature setting that corresponds to the event is enabled. Sensors generate events for only those signatures that are enabled. These events are then received by the Security Monitor server.

You can also generate audit reports. The audit reports provide information about system events. The following sections describe the types of reports and how to generate and access reports:

- Understanding the Types of Reports, page 6-2
- Scheduling and Generating Reports, page 6-5
- Viewing Reports, page 6-7
- Exporting a Report, page 6-7
- Deleting Generated Reports, page 6-8
- Editing Report Parameters, page 6-9
- Deleting Scheduled Report Templates, page 6-10

ECT 5264 CPL - AC

Understanding the Types of Reports

You can view two categories of reports in Security Monitor: alarm reports and audit reports. Alarm reports provide information about the events being collected by Security Monitor. Audit reports provide information about Security Monitor system events.

Both types of reports can be generated on-demand or scheduled for a later date and time. You can configure scheduled reports to repeat at regular intervals.

The following sections describe the different report types:

- About Alarm Reports, page 6-2
- About Audit Reports, page 6-4
- About Scheduled Reports, page 6-5

About Alarm Reports

You can generate the following alarm reports in Security Monitor:

- **Security Alarm Source Report**—Summarizes alarms received on the syslog port by the source of the events. For example, if Security Monitor receives alarms from a PIX Firewall, use this report to view the alarm information. Filterable by Event Level, Source IP Address, and Time/Date.
- **Security Alarm Detailed Report**—Provides detailed information for each security alarm received. Filterable by Event Level, Source IP Address, and Time/Date.
- **IDS Top Sources Report**—Reports the specified number of source IP addresses that have generated the most events during a specified time period. Filterable by Date/Time, Top *n*, where *n* is the number of sources, Destination Direction, Destination IP Address, Signature or Signature Category, Sensor, and Event Level.
- **IDS Top Source/Destination Pairs Report**—Reports the specified number of source/destination pairs (that is, connections or sessions) that have generated the most alarms during a specified time period. Filterable by Date/Time, Top *n*, where *n* is the number of source/destination pairs, Signature or Signature Category, Sensor, Event Level, Source Direction, Destination Direction, Source Address, and Destination Address.

RQS N° 03/2005 - CN
CPMI - CORREIOS
1305
Fls:
Doc: 3701

E C T
5263
C P L Porta A

- **IDS Top Destinations Report**—Reports the specified number of destination IP addresses that have been targeted for attack during a specified time period. Filterable by Date/Time, Top *n*, where *n* is the number of destinations, Source Direction, Source Address, Signature or Signature Category, Sensor, and Event Level.
- **IDS Top Alarms Report**—Reports the specified number of top alarms, by signature name, that have been generated during a specified time period. Filterable by Date/Time, Top *n*, where *n* is the number of alarms, Source Direction, Destination Direction, Source Address, Destination Address, Signature or Signature Category, Sensor, Event Level, and Signature or Signature Category.
- **IDS Summary Report**—Provides a summary of event information for an organization during a specified time period. Filterable by Date/Time, Organization, Source Direction, Destination Direction, Signature or Signature Category, and Event Level.
- **IDS Alarms by Sensor Report**—Reports logged alarms based on the sensor (Host ID) that detected the event. Filterable by Date/Time, Source Direction, Destination Direction, Source Address, Destination Address, Signature or Signature Category, Sensor, Event Level, and Event Count.
- **IDS Alarms by Hour Report**—Reports alarms in one-hour intervals over the time specified by the user. Filterable by Date/Time, Source Direction, Destination Direction, Source Address, Destination Address, Signature or Signature Category, Sensor, Event Level, and Event Count.
- **IDS Alarms by Day Report**—Reports alarms in one-day intervals over the time specified by the user. Filterable by Date/Time, Source Direction, Destination Direction, Source Address, Destination Address, Signature or Signature Category, Sensor, Event Level, and Event Count.
- **IDS Alarm Source/Destination Pair Report**—Reports logged alarms based on source/destination IP address pairs (that is, connections or sessions). Filterable by Date/Time, Signature or Signature Category, Sensor, Event Level, Alarm Count, Source Direction, Destination Direction, Source Address, and Destination Address.
- **IDS Alarm Source Report**—Reports alarms based on the source IP address that generated the alarm. Filterable by Date/Time, Destination Direction, Destination Address, Signature or Signature Category, Sensor, Event Level, Alarm Count, Source Direction, and Source Address.

RC 2005 - CN
CPMI - CORREIOS
Fls: 1306
Doc: 3701

ECT 5262 CPL - AC

- **IDS Alarm Report**—Reports logged alarms based on signature names. Filterable by Date/Time, Source Direction, Destination Direction, Source Address, Destination Address, Sensor, Event Level, Event Count, and Signature or Signature Category.
- **IDS Alarm Destination Report**—Reports alarms based on the destination IP address that generated the alarm. Filterable by Date/Time, Source Direction, Source Address, Signature or Signature Category, Sensor, Event Level, Event Count, Destination Direction, and Destination Address.
- **Daily Metrics Report**—Reports event traffic totals, by day, from the selected date until the current date. Reporting occurs in 24-hour intervals, starting at midnight. The report shows events by platform (PIX, IOS, Sensor, RDEP) and event type (IDS or Security).
- **24 Hour Metrics Report**—Reports all alarm traffic from the most recent 24 hours in 15 minute intervals. There are no filters for this report.

About Audit Reports

Audit reports provide information about management server events. If IDS MC and Security Monitor are installed on the same server, the generated audit reports and scheduled audit report templates are shared between the applications.

The following audit reports are available:

- **Subsystem Report**—Reports audit records ordered by the IDS subsystem, which includes systems from IDS MC and Security Monitor and systems common to each. Filterable by Event Severity, Date/Time, and Subsystem.
- **Sensor Version Import Report**—Reports the audit records that are generated when the version identifier of IDS sensor devices is imported into IDS MC. These records indicate success or failure of the import operation. Filterable by Device, Event Severity, and Date/Time.
- **Sensor Configuration Import Report**—Reports the audit records that are generated when you import IDS Sensor configurations into IDS MC. The resulting records can be used to determine success or failure in device configuration import tasks. Filterable by Device, Event Severity, and Date/Time.

78-15616-01
RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1307
Doc: 3791

ECT 1 5261 Comum CPL - AC

- **Sensor Configuration Deployment Report**—Reports records related to IDS sensor configurations deployed to devices using IDS MC. These records indicate successful deployment or provide error messages where appropriate for deployment operations. Filterable by Device, Event Severity, and Date/Time.
- **Console Notification Report**—Reports the console notification records generated by the notification subsystem. Filterable by Event Severity and Date/Time.
- **Audit Log Report**—Reports audit records by the server and application. Unlike the other report templates, this report template provides a broad, non-task-specific view of audit records in the database. Filterable by Task Type, Event Severity, Date/Time, Subsystem, and Applications.

About Scheduled Reports

For each report type that you choose to generate, you can enter a report title, schedule, and notification options. Enter this information in the Schedule Report page when you select **Reports > Generate**. You can run the report immediately, or you can schedule the report to run at a later time, at regular intervals, or both.

If you choose to run the report at a later time, you must specify the date and time that you want the report to run. Additionally, you can schedule the report to run at regular intervals, such as hourly, daily, or weekly. You can edit the report parameters of a scheduled report on the Edit Scheduled Reports page, which you access by selecting Reports > Scheduled. You can also delete scheduled report templates from this page.

Each time a scheduled report is run, it is added to the Completed Report page.

Scheduling and Generating Reports

On the Select Report page, you can select the type of report to generate and define the parameters for the selected report. Based on the scheduling parameters you select, the report runs immediately, at a later time, or at regular intervals.

RQS 6-5 CPMI - CORREIOS 1308 Fls: Doc: 3791

To generate a report, follow these steps:

Step 1 Select **Reports > Generate**.

Result: The Select Report page appears.

Tip In Security Monitor, you can filter which reports appear on the page. From the Report Group list, select **All** to show both alarm and audit reports, **Alarms** to show only alarm reports, or **Audit** to show only audit reports.

Step 2 Select the report type that you want to generate, and then click **Select**.

Result: The Report Filtering page appears.

Step 3 Enter the report parameters for the report type you selected. Then, click **Next**.

Result: The Schedule Report page appears.

Step 4 Enter a name for the report in the Report Title field.

Step 5 Click the **Run Now** or **Schedule for Later** radio button under Schedule Options. If you select Run Now, skip to Step 7. If you select Schedule for Later, specify the following options:

a. Specify the date and time that you want the report to run in the Start Time list boxes. The date is specified by month, day, and year. The time is specified in hours and minutes. The time zone used to determine the time is to the right of the Start Time list boxes.

b. To run the report at regular intervals, select an option in the Repeat every list box. You can schedule the report to run every day, week, weekday, weekend day, hour, or minute.

Step 6 To send an e-mail notification to someone when the report runs, select the **Email report to** check box and enter an e-mail address in the adjacent field. Use commas to separate multiple addresses. Then, click **Finish**.

Result: If you select Run Now, the report runs and you can view the generated report by selecting Reports > View. If you select Schedule for Later, you can view the scheduled report template by selecting Reports > Scheduled.

ECT 5260 La Paz AC
CPMI - CORREIOS
Fls: 1309
Doc: 3701

ECT 5249 Paula PL - AC

Viewing Reports

After you generate a report, you can view it.

To view a report, follow these steps:

Step 1 Select **Reports > View.**

Result: The Choose Completed Report page appears.

Tip In Security Monitor, you can filter which reports appear on the page. From the Report Group list, select **All** to show both alarm and audit reports, **Alarms** to show only alarm reports, or **Audit** to show only audit reports.

Step 2 Select the check box corresponding to the title of the report you want to view.

Step 3 To view the selected report, click **View.**

Result: The report appears in the Report page.

Step 4 To view the report in a new browser window, click **Open in Window. . ..**

Result: The report appears in a new browser window.

Exporting a Report

After you generate a report, you can export that report to an HTML file.

To export a report, follow these steps:

Step 1 Select **Reports > View.**

Result: The Choose Completed Report page appears.

Tip In Security Monitor, you can filter which reports appear on the page. From the Report Group list, select **All** to show both alarm and audit reports, **Alarms** to show only alarm reports, or **Audit** to show only audit reports.

RQS 6-7 5 - CN
CPMI - CORREIOS
1310
Fls:
3701
Doc:

ECT 5248 Fls: AC

Step 2 To select the report that you want to export, select the check box corresponding to the report title.

Step 3 Click **Open in Window**.

Result: If you are using Internet Explorer, the report appears in a new browser window; proceed to Step 4. If you are using Netscape Navigator, the Unknown File Type dialog box appears; skip to Step 5.

Step 4 To save the report, select **File > Save As** from the Internet Explorer menu bar. Browse to the location where you want to save the file and enter a filename. Then, click **Save**.

Result: The report is saved using the filename and location you specified.

Skip Step 5.

Step 5 To save the report, click **Save File**. Browse to the location where you want to save the file and enter a filename. Then, click **Save**.

Result: The report is saved using the filename and location you specified.

Deleting Generated Reports

You can delete generated reports. If the report was generated from a scheduled report template, deleting the report does not delete the associated scheduled report template.

To delete a report, follow these steps:

Step 1 Select **Reports > View**.

Result: The Choose Completed Report page appears.

Tip In Security Monitor, you can filter which reports appear on the page. From the Report Group list, select **All** to show both alarm and audit reports, **Alarms** to show only alarm reports, or **Audit** to show only audit reports.

03/2005 - CN
CPMI - CORREIOS
Fls: 1311
3701
Doc:

E C T
5247
PL - AC

Step 2 Select the check box next to the title of the report you want to delete.

Tip You can delete more than one report at a time. To delete more than one report, select the check boxes next to all reports that you want to delete.

Result: A check mark appears next to each report you selected.

Step 3 To delete the selected report, click **Delete**.

Result: The report is deleted. The report name is removed from the list of available reports.

Editing Report Parameters

You can edit the report parameters or the schedule for a scheduled report template.

To edit the report parameters, follow these steps:

Step 1 Select **Reports > Scheduled**.

Result: The Edit Scheduled Reports page appears.

Tip In Security Monitor, you can filter which reports appear on the page. From the Report Group list, select **All** to show both alarm and audit reports, **Alarms** to show only alarm reports, or **Audit** to show only audit reports.

Step 2 Select the check box corresponding to the title of the report template that you want to edit.

Result: A check mark appears next to the report you selected.

Step 3 To open the selected report template, click **Edit**.

Result: A new page displays the report parameters. Depending on the type of report, the parameters are different.

6-9
2005 - CN
CPMI - CORREIOS
1312
Fls:
3701
Doc:

ECT 5246 Folha 19 CPL - AC

Step 4 Change any report parameters that you want to. To save your changes, click **Finish**.

Result: The changes you made are saved to the report template.

Deleting Scheduled Report Templates

You can delete unwanted scheduled report templates. Deleting a scheduled report template also deletes all associated reports that have already been generated.

To delete a scheduled report template, follow these steps:

Step 1 Select **Reports > Scheduled**.

Result: The Edit Scheduled Reports page appears.

Tip In Security Monitor, you can filter which reports appear on the page. From the Report Group list, select **All** to show both alarm and audit reports, **Alarms** to show only alarm reports, or **Audit** to show only audit reports.

Step 2 Select the check box corresponding to the title of the report you want to delete.

Tip You can delete more than one report template at a time. To do so, select the check boxes corresponding to all the report templates that you want to delete.

Result: A check mark appears next to each report you selected.

Step 3 To delete the report template, click **Delete**.

Result: The selected report template and all associated end reports are deleted.

78-15616-01
RGS Nº 03/2005 - CN
CPMI - CORREIOS
1313
Fls:
Doc: 3701

Apêndice CZ

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1314
Doc: 3701

IDS Device Manager Configuration Tasks

After configuring system information, you are ready to configure signatures, set up blocking, set up automatic signature updates, and restore defaults.

The following sections describe how to configure these options through the Configuration tab:

- Configuring Signatures, page 3-1
- Configuring Blocking, page 3-20
- Configuring Automatic Updates, page 3-35
- Restoring Default Settings, page 3-38

Configuring Signatures

You can create system variables, create event filters, and tune signatures through the Sensing Engine.

The following sections describe how to configure signatures through the Sensing Engine:

- Explaining Signatures, page 3-2
- Configuring Alarm Channel System Variables, page 3-3
- Configuring Alarm Channel Event Filters, page 3-6
- Configuring Virtual Sensor System Variables, page 3-9
- Working with Virtual Sensor Signature Configuration Mode, page 3-12
- Identifying Traffic Oversubscription, page 3-19

Explaining Signatures

Attacks or other misuses of network resources can be defined as network intrusions. Network intrusions can be detected by sensors that use a signature-based technology. A signature is a set of rules that your sensor uses to detect typical intrusive activity, such as denial of service (DoS) attacks. As sensors scan network packets, they use signatures to detect known attacks and respond with actions that you define.

The sensor compares the list of signatures with network activity. When a match is found, the sensor takes an action, such as logging the event or sending an alarm to IDS Event Viewer. Sensors allow you to modify existing signatures and define new ones.

Signature-based intrusion detection can produce false positives because certain normal network activity can be misinterpreted as malicious activity. For example, some network applications or operating systems may send out numerous ICMP messages, which a signature-based detection system might interpret as an attempt by an attacker to map out a network segment. You can minimize false positives by tuning your sensors.

To configure a sensor to monitor network traffic for a particular signature, you must enable the signature. By default, the most critical signatures are enabled when you install IDS Device Manager. When an attack is detected that matches an enabled signature, the sensor generates an alert event (formerly known as an alarm), which is stored in the sensor's event store. The alert events, as well as other events, may be retrieved from the event store by web-based clients. By

ECT 5243 Paulica CPL - AC

default the sensor logs all Informational alarms or higher. If you have added IDS Event Viewer as a destination, the alarm is sent to the IDS Event Viewer database and you can view the alarm in IDS Event Viewer.

Some signatures have subsignatures, that is, the signature is divided into subcategories. When you configure a subsignature, changes made to the parameters of one subsignature apply only to that subsignature. For example, if you edit signature 3050 subsignature 1 and change the severity, the severity change applies to only subsignature 1 and not to 3050 2, 3050 3, and 3050 4.

Built-in signatures are known attack signatures that are included in the sensor software and are enabled by default. You cannot add to or delete from the list of built-in attack signatures. You also cannot rename them. You can tune built-in signatures by adjusting several signature parameters. Built-in signatures that have been modified are called *tuned* signatures.

You can create new signatures, which are called *custom* signatures. Custom signature IDs begin at 20000. You can configure them for any number of things, such as matching of strings on UDP connections, tracking of network floods, and scans. Each signature is created using a signature engine specifically designed for the type of traffic being monitored.

Configuring Alarm Channel System Variables

Alarms are sent to the alarm channel, where they are filtered and aggregated. You cannot select the alarm channel, because there is only one alarm channel in version 4.0.

You can change the value of an alarm channel system variable, but you cannot add variables or delete variables. You also cannot change the name, type, or constraints of a variable.

For all the Sensing Engine panels, you must click the **Save Changes** icon on the Activity bar to apply your new configuration.

You use the system variables when configuring alarm channel event filters. When you want to use the same value within multiple filters, use a variable. When you change the value of a variable, the variables in all the filters are updated. This saves you from having to change the variable repeatedly as you configure alarm filters. See Configuring Alarm Channel Event Filters, page 3-6, for more information.

CPMI CORREIOS
1316
Fls:
3701
Doc:

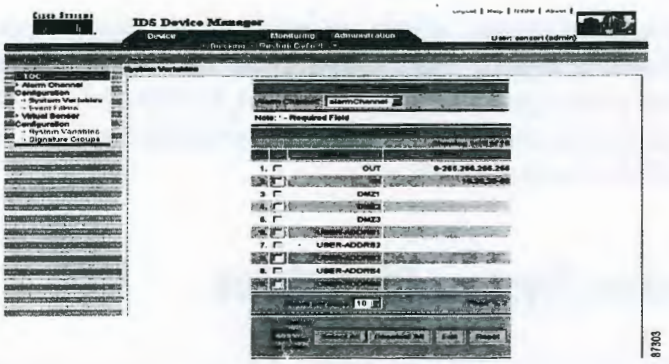
For example, if you had an IP address space that applied to your engineering group and there were no Windows systems in that group, and you were not worried about any Windows-based attacks, you could set up a USER-ADDR1 to be the engineering group's IP address space. You could then use this variable on the Event Filters page to set up the filter to ignore all Windows-based attacks for USER-ADDR1.

To define alarm channel system variables, follow these steps:

Step 1 Select **Configuration > Sensing Engine > Alarm Channel Configuration > System Variables.**

The System Variables page appears.

Figure 3-1 System Variables Page

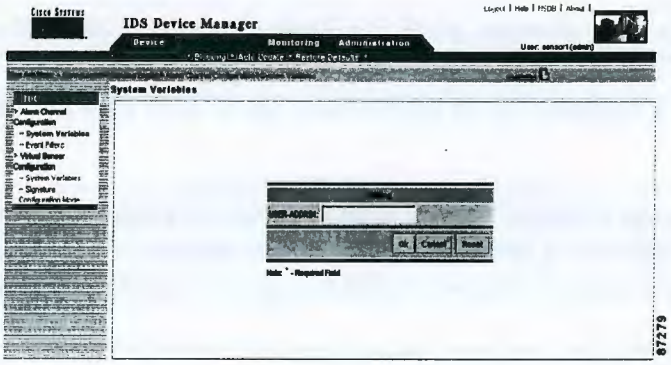


Step 2 Select the check box next to the system variable you want to edit, and then click **Edit.**

The Editing page appears for the variable that you chose.

Note You can edit only one variable at a time. You can adjust the page view using the Rows per page list box at the bottom of the page, or you can move to additional pages of variables by selecting a page from the Page list box.

Figure 3-2 Editing Page



Step 3 Fill in the following values for the following system variables (according to the one that you are editing):

- OUT

  OUT is defined as anything that is not included in IN. You cannot edit this variable. The default is 0–255.255.255.255.

- IN

  IN is a list of all internal IP address spaces. Enter your internal IP addresses.

- DMZ1, DMZ2, and DMZ3

  You can use DMZ to define any valid IP address. These are named DMZ for you to use with filtering signatures that pertain to firewalls.

- USER-ADDRS1, USER-ADDRS2, USER-ADDRS3, USER-ADDRS4, and USER-ADDRS5

  You can use USER-ADDR to define any valid IP address. You can set up a USER-ADDR variable to apply to any group of IP addresses that you want to use a filter on.

- SIG1, SIG2, SIG3, SIG4, and SIG5

  You can use SIG to define popular signatures that you like to exclude for certain addresses.

Note To reset the form, click **Reset**.

Step 4 Click **Ok**.

Note To undo your changes, click the **Undo Changes** icon on the Activity bar.

Step 5 Click the **Save Changes** icon in the Activity bar to save your system variables.

Note A message displays "Configuration update in progress. This page will be unavailable for a few minutes." In a few minutes, click **Alarm Channel Configuration > System Variables** again to see the edited variable in the list.

The new value appears in the Value column.

Step 6 Repeat Steps 2 though 5 to edit additional system variables.

Configuring Alarm Channel Event Filters

You can configure event filters that are based on source and destination addresses for specified signatures. You can use the alarm channel system variables that you defined on the Alarm Channel System Variables page to group addresses for your filters.

For all the Sensing Engine panels, you must click the **Save Changes** icon on the Activity bar to apply your new configuration.

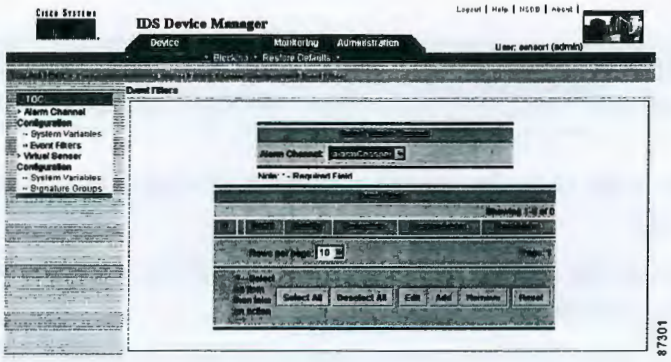
E C T
5239
Paulo
S/SL - AC

To configure alarm channel event filters, follow these steps:

Step 1 Select **Configuration > Sensing Engine > Alarm Channel Configuration > Event Filters**.

The Event Filters page appears.

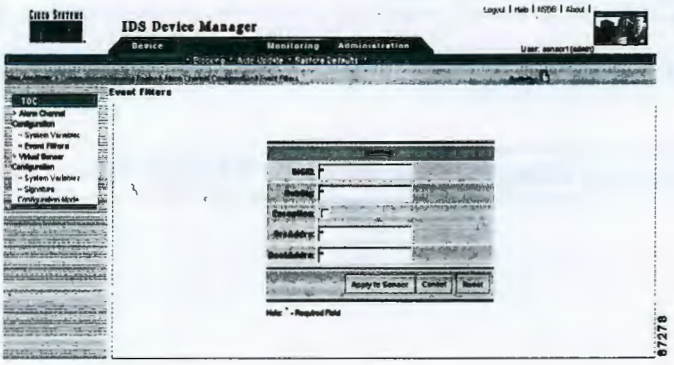
Figure 3-3 Event Filters Page



Step 2 Click **Add** to add an event filter.

The Adding page appears.

Figure 3-4 Adding Page



RQS Nº 3.7 CN
CPMI - CORREIOS
1318
Fls:
3701
Doc:

Step 3 In the SIGID field, enter the signature IDs of the events to which this filter should be applied.

You can use a list (2001, 2004), or a range (2001–2004), an asterisk (*) for all signatures, or one of the SIG variables if you defined them on the Alarm Channel System Variables page.

Step 4 In the SubSig field, enter the subsignature IDs of the events to which this filter should be applied.

Step 5 In the Exception field, enter the exception (Boolean) to the event filter.

Note If the filter describes an exception to an event filter, you can create a "general case" exclusion rather than adding more specific information.

Step 6 In the SrcAddrs field, enter the source addresses of events to which this filter should be applied.

You can use one of the DMZ or USER-ADDR variables if you defined them on the Alarm Channel System Variables page.

Step 7 In the DestAddrs field, enter the destination addresses of events to which this filter should be applied.

You can use one of the DMZ or USER-ADDR variables if you defined them on the Alarm Channel System Variables page.

Note To reset the form, click **Reset**.

Step 8 Click **Apply to Sensor**.

Note To undo your changes, click the **Undo Changes** icon on the Activity bar.

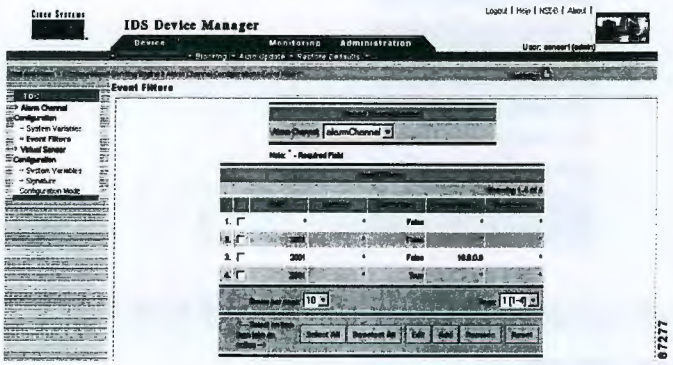
ECT 5237 Paula CPL - AC

Step 9 Click **Saves Changes** on the Activity bar to save your changes.

Note A message displays "Configuration information is not available at this time. Try again in a few minutes." After a few minutes, click **Event Filters** again to see the filter you added.

The filtered signature appears on the Event Filters page.

Figure 3-5 Added Event Filters Page



Step 10 To remove the filter, select the check box next to the signature and click **Remove**.

Configuring Virtual Sensor System Variables

You can change the value of a system variable but you cannot add variables or delete variables. You cannot change the name or type of a variable. You cannot select the virtual sensor, because there is only one virtual sensor in version 4.0.

RQS N 3-9 CN CPMI CORREIOS Fls: 1319 Doc: 3701

To configure the virtual sensor system variables, follow these steps:

Step 1 Select **Configuration > Sensing Engine > Virtual Sensor Configuration > System Variables**.

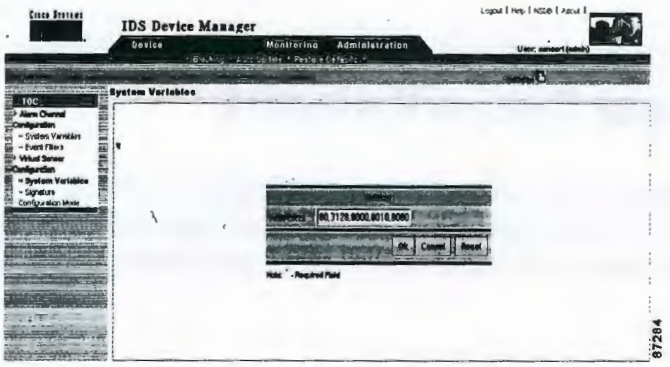
The System Variables page appears.

Figure 3-6 System Variables Page

Step 2 Select the system variable that you want to edit and click **Edit**.

The Editing page appears.

Figure 3-7 Editing Page



E C T
1 5235
Fls:
CPL - AC

Step 3 Fill in the value of the system variable that you want to edit:

Note You can edit only one system variable at a time. You can adjust the page view using the Rows per page list box at the bottom of the page, or you can move to additional pages of variables by selecting a page from the Page list box.

- WEBPORTS

  WEBPORTS has a predefined set of ports where web servers are running, but you can edit the value. This variable affects all signatures that have web ports. The default is 80, 3128, 8000, 8010, 8080, 8888, 24326.

- Ports1, Ports2, Ports3, Ports4

  You can set up a list of ports to apply to particular signatures.

- ADDRS1, ADDRS2, ADDRS3, ADDRS4

  You can set up this variable with a list of addresses to use anywhere you can use IP addresses.

- IPReassembleMaxFrags

  You can define the total number of fragments you want the system to queue. You can define a number between 1000 and 50,000. The default is 10,000.

Note To reset the form, click **Reset**.

Step 4 Click **OK**.

Note To undo your changes, click the **Undo Changes** icon on the Activity bar.

CPMI - 3-11
1320
Fls:
Doc: 3701

Step 5 Click the **Save Changes** icon on the Activity bar to save your system variables.

Note A message displays "Configuration update in progress. This page will be unavailable for a few minutes." After a few minutes, click **Virtual Sensor Configuration > System Variables** to see the edited variable.

The new value appears in the Value column.

Step 6 Repeat Steps 2 though 5 to edit additional system variables.

Working with Virtual Sensor Signature Configuration Mode

The Signature Configuration Mode page displays a list of top level categories of signature groups for the virtual sensor. You can see all the signatures in the list or you can see signatures that are grouped according to their signature engine type. Certain signatures are enabled by default to provide you immediately with a certain level of security. When you modify a built-in signature, it becomes a tuned signature. You can also create signatures, which are called custom signatures.

You cannot select the virtual sensor, because there is only one virtual sensor in version 4.0.

You can display all individual signatures at once by clicking **All Signatures**. If you are looking for a particular signature, click **All Signatures**, and use the browser's search option to find the string you are looking for—the signature ID or the signature name.

You can display the signature list within a group by clicking the group name. Each group displays its enable level (the disabled, partially enabled, or enabled icon). You can enable or disable one, some, or all signatures within the group. To select the signature for enabling or disabling, select the signature check box.

You can tune built-in signatures. To tune a signature, select the check box and click **Edit**. Some signatures have subsignatures, which you can edit individually to have more control over the signature. You can create custom signatures, and then delete one, some, or all custom signatures. To create a custom signature, choose the correct signature engine, and then click Add and configure the signature parameters. For more information on signature engines and their parameters, see Appendix A, "Working With Signature Engines."

A signature can be in multiple groups. Editing a signature in one group, affects it in all groups. For example, if you enable all general attack signatures in the Attack category, it will enable 7107. If you disable the ATOMIC.ARP signature in the Engine category, 7107 will be disabled. Whichever action is the last one, is the one that is applied.

To configure virtual sensor signature groups, follow these steps:

Step 1 Select **Configuration > Sensing Engine > Virtual Sensor Configuration > Signature Configuration Mode**.

The Signature Groups page appears.

Figure 3-8 Signature Groups Page

Step 2 To enable or disable all signatures in a group, select the check box next to the signature group, and then click **Enable** or **Disable**.

Note A clear circle indicates that no signatures in that signature group are enabled. A solid circle indicates that all signatures are enabled. A partial circle indicates that at least one signature in that group is enabled.

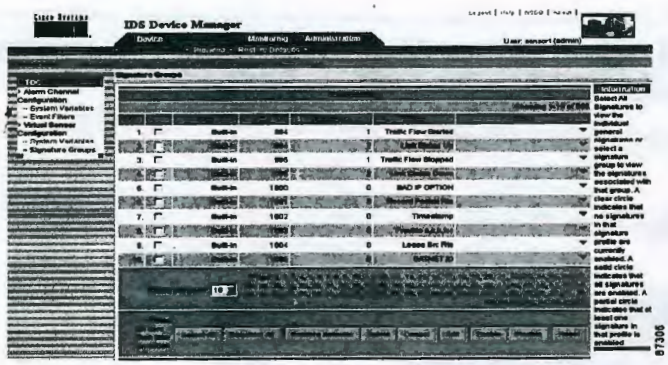
Note Click **Restore Defaults** to return the signature group to its default settings.

Step 3 You can click **All Signatures** to display all the IDS signatures or you can click a signature group name.

The All Signatures page appears.

Note If you select **All** in the Rows per page list box, it can take some time for all signatures to display.

Figure 3-9 All Signatures Page



The All Signatures page contains the following:

- Enabled or Disabled icon
- Signature ID
- Subsignature ID
- Signature name
- Type (built-in, tuned, custom)
- Severity level (Informational, Low, Medium, High)
- Action
- More (lists all the signature parameters; these appear when you edit the signature)

ECT 5231 Paulo PL - AC

Step 4 Select the check box(es) next to the signatures that you want to perform an action on:

Note You can edit only one signature at a time. You can adjust the page view using the Rows per page list box at the bottom of the page, or you can move to additional pages of variables by selecting a page from the Page list box.

- To enable or disable the signature(s), click **Enable** or **Disable**.

Caution Signatures can belong to more than one group. Enabling or disabling signatures in one group also affects those signatures that belong to other groups.

- To restore the defaults to a signature(s), click **Restore Defaults**.
- To delete a signature(s), click **Delete**.

Note You cannot delete built-in or tuned signatures, only custom signatures.

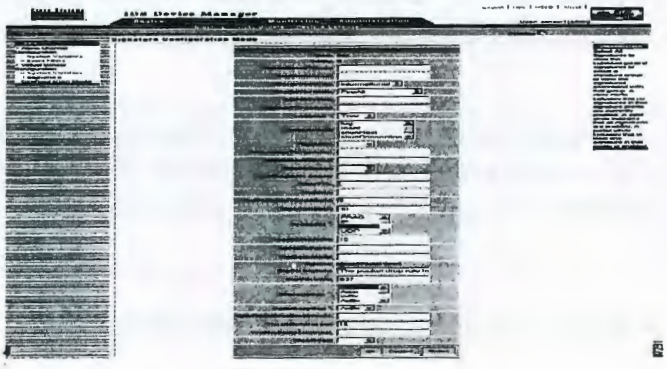
- To edit the signature(s), click **Edit**.

The Editing page appears.

This is where you tune built-in signatures. You can see the definition of each parameter by passing your mouse over the parameter. Some parameters are required (red asterisk), others have menu lists you can choose from, for others you must add text. For a detailed description of signature engines and parameters, see Appendix A, "Working With Signature Engines."

CPMI - C 3-15
1322
Fls:
Doc: 3701

Figure 3-10 Editing Page



Step 5 Click **Ok** to save the changes you made to the built-in signature.

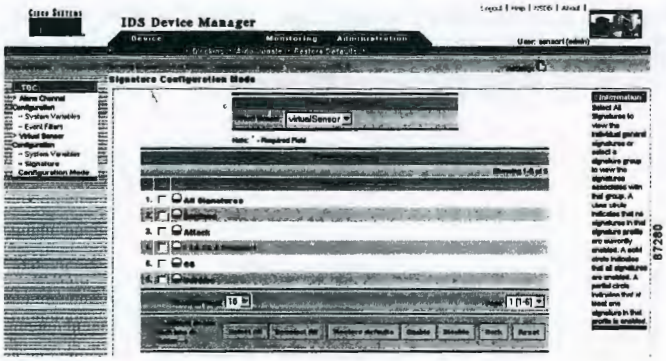
The Type has changed from Built-in to Tuned on the All Signatures page.

Note Use the **Back** button at the bottom of the page as you tune or create multiple signatures.

Note To undo your changes, click the **Undo Changes** icon on the Activity bar.

Step 6 To create a custom signature, click the Engines category on the Signature Groups page.

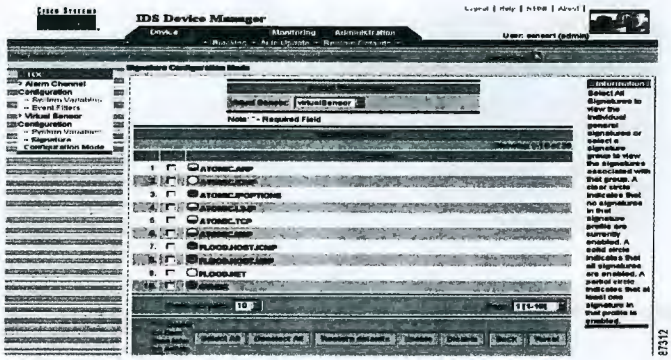
Figure 3-11 Signature Groups Page



ECT 1 3229 Baiba L-AC

The Engines page appears.

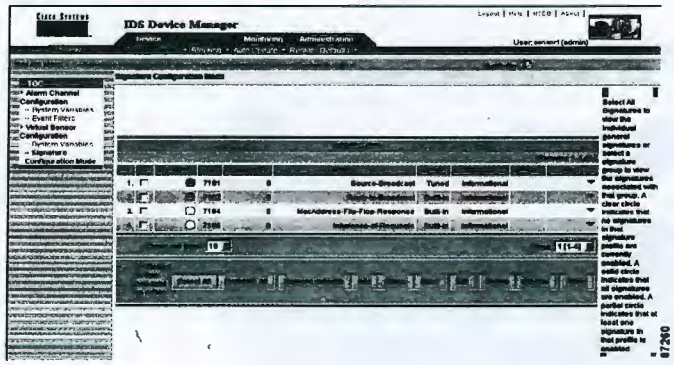
Figure 3-12 Engines Page



Step 7 Click the engine you want to use to create a custom signature, for example, **ATOMIC.ARP**.

The ATOMIC.ARP page appears.

Figure 3-13 ATOMIC.ARP Page

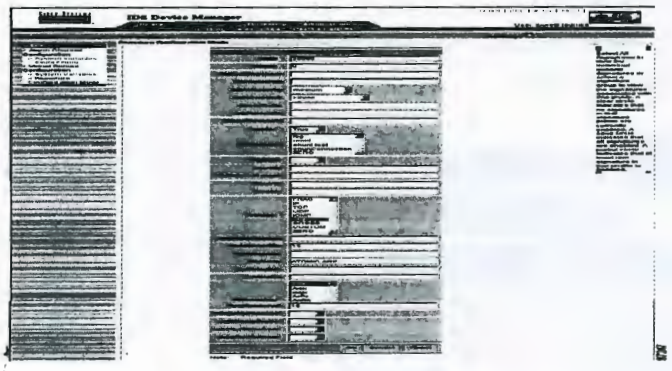


Step 8 Click **Add**.

The Adding page appears.

CPMI - CORREIOS
1323
Fls:
3701
Doc:

Figure 3-14 Adding ATOMIC.ARP Page

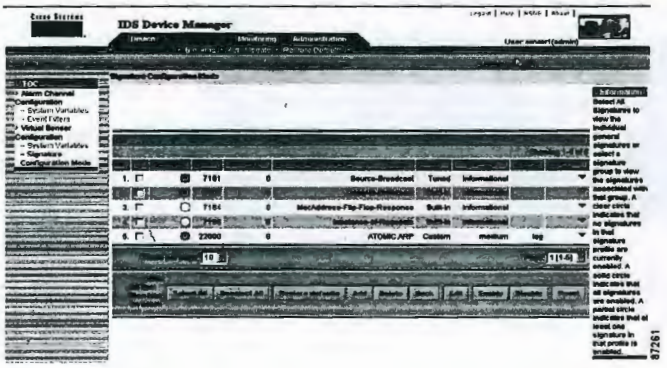


Step 9 Fill in the parameters that you want, and then click **OK**.

Note For a detailed description of signature engines and parameters, see Appendix A, "Working With Signature Engines."

A note tells you that to add the signature you must click **Save Changes** on the Activity bar (see Step 10). The ATOMIC.ARP page appears with the custom signature in the list.

Figure 3-15 ATOMIC.ARP Page with Custom Signature



E C T
1 5227
Fls
C P L - A C

Step 10 Click the **Save Changes** icon on the Activity bar to save your changes.

Note A message displays "Configuration update in progress. This page will be unavailable for a few minutes." Click **Virtual Sensor Configuration > Signature Configuration Mode** to return to the Signature Configuration Mode page. Click **All Signatures** or the relevant signature group to see the tuned signature in the list.

The built-in signature that you edited now shows Tuned in the Type column.

Identifying Traffic Oversubscription

Signature 993 alarms tell you if the sensor is dropping packets and the percentage dropped to help you tune the traffic level you are sending to the sensor. For example, if the alarms show that there is zero or a very small percentage of dropped packets, the sensor is able to monitor the quantity of traffic being sent.

If you are seeing 993 alarms with a higher percentage of dropped packets, your sensor is oversubscribed. When a sensor gets oversubscribed, it can have difficulty in detecting alarms in TCP streams in a nonlinear fashion. The percentage of streams that are affected by the dropped packets is not easy to predict. If you find that you are operating your sensor in an environment where it is oversaturated and you need to continue operating it in that environment, we recommend disabling the TCP3WayHandshake and setting TCPReassemblyMode to loose so that best security is ensured.

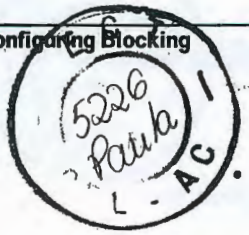
Signature 993, which is part of the signature engine OTHER, has the following configuration parameters:

- MpcInterval in seconds 5 <= MpcInterval <= 2500 (default = 30).

  MpcInterval is the interval between alarms.
- MpcPercentThreshold in percent 0 <= MpcPercentThreshold <= 100 (default = 0).

  MpcPercentThreshold is the percentage of missed packets that must be exceeded to trigger an alarm. A value of 100 percent disables this threshold.

CPMI - 3-19
1324
Fls:
Doc:
5701



- MpcAbsThreshold in packets 0 <= MpcAbsThreshold <= 65535 (default = 0).

  MpcAbsThreshold is the absolute number of missed packets that must be exceeded to trigger an alarm. A value of 65535 disables this threshold.

If either the MpcPercentThreshold or the MpcAbsThreshold is exceeded, the alarm is triggered.

Note If signature 993 is firing with 100 percent packet loss, the sensor is not generating alarms and there is a problem. Make sure that you have the most recent version of the sensor. If you have the most recent version, contact TAC to report the problem.

See OTHER Engine, page A-30, for more information on the OTHER signature engine.

Configuring Blocking

You can configure a sensor to block an attack by generating ACL rules for publication to a Cisco IOS router, or a Catalyst 6500 family switch, or by generating shun rules on a PIX Firewall.

The following sections describe how to set up blocking:

- Configuring Blocking Properties, page 3-21
- Configuring Addresses Never To Block, page 3-22
- Setting Up Logical Devices, page 3-24
- Configuring Blocking Devices, page 3-26
- Configuring Router Blocking Device Interfaces, page 3-28
- Configuring Catalyst 6K Blocking Device Interfaces, page 3-30
- Configuring a Master Blocking Sensor, page 3-31
- Setting Up a Blocking Forwarding Sensors, page 3-33

Configuring Blocking Properties

You set up global blocking properties for the Network Access Controller (NAC) on this page. NAC is responsible for controlling blocking actions on managed devices.

To configure blocking on the sensor, follow these steps:

Step 1 Select **Configuration > Blocking Properties**.

The Blocking Properties page appears.

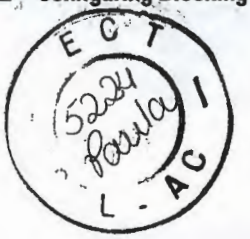
Figure 3-16 Blocking Properties Page

Step 2 Do not select the Allow the Sensor IP to be Blocked check box unless necessary.

Caution We suggest that you do not allow the sensor to block itself, because it will stop communicating with the managed device. You can select this option if you can ensure that if the sensor creates a rule to block its own IP address, it will not prevent the sensor from accessing the blocking device.

Step 3 In the Maximum Block Entries field, enter how many blocks are to be maintained simultaneously (0 to 250).

Note We do not recommend or support setting the maximum block entries higher than 250.



The default value is 100.

Note The number of blocks will not exceed the maximum block entries. If the maximum is reached, new blocks will not occur until existing blocks time out and are removed.

Note To reset the form, click **Reset**.

Step 4 Click **Apply to Sensor** to save your changes.

Configuring Addresses Never To Block

You must tune your sensor to identify hosts and networks that should never be blocked, not even manually, because you may have a trusted network device whose normal, expected behavior appears to be an attack. But such a device should never be blocked, and trusted, internal networks should never be blocked. Properly tuning signatures reduces the number of false positives and helps ensure proper network operations. Tuning and filtering signatures prevents alarms from being generated. If an alarm is not generated, the associated block does not occur.

If you specify a netmask, this is the netmask of the network that should never be blocked. If no netmask is specified, only the IP address you specify will never be blocked.

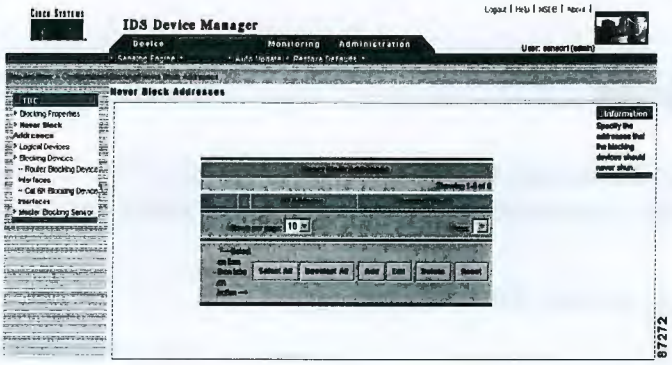
E C
5223
Fls: 1
CPMI - CORREIOS

To set up addresses never to be blocked by blocking devices, follow these steps:

Step 1 Select **Configuration > Never Block Addresses.**

The Never Block Addresses page appears.

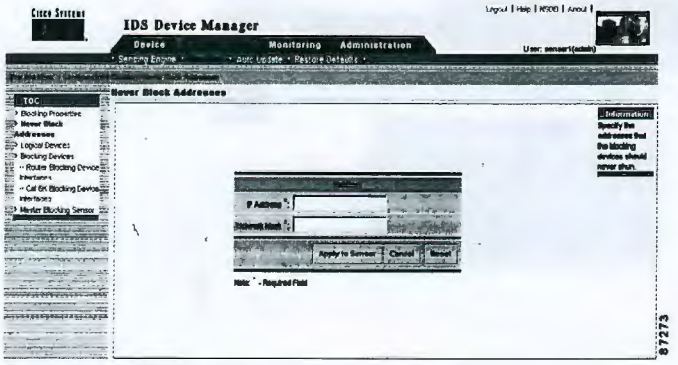
Figure 3-17 Never Block Addresses Page



Step 2 Click **Add** to add addresses that should never be blocked.

The Adding page appears.

Figure 3-18 Adding Page



Step 3 In the IP Address field, enter the IP address of the host that should never be blocked.

DOC Nº 03/2005 - CN
CPMI - CORREIOS
3-23
1326
Fls:
3701
Doc:

Step 4 In the Network Mask field, enter the network mask of the network that should never be blocked.

Note To reset the form, click **Reset**.

Step 5 Click **Apply to Sensor** to save your changes.

Setting Up Logical Devices

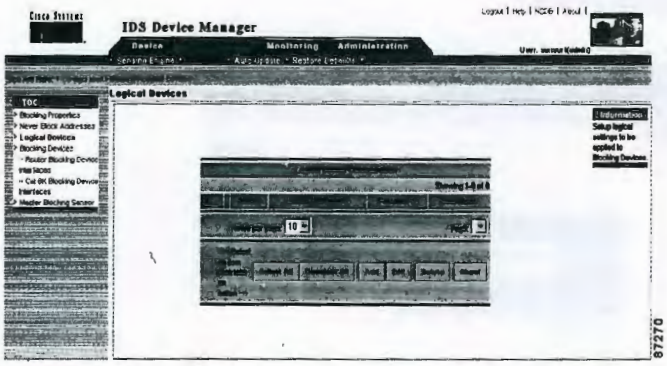
You can add logical devices that the senor will manage. For example, routers that all share the same passwords and usernames can be under one logical device name.

To set up logical devices, follow these steps:

Step 1 Select **Configuration > Logical Devices**.

The Logical Devices Configuration page appears.

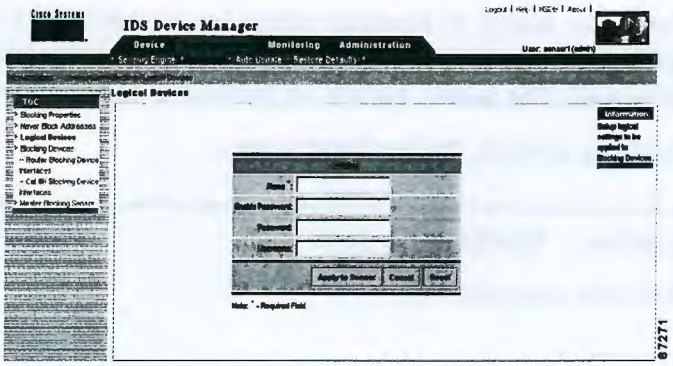
Figure 3-19 Logical Device Configuration Page



Step 2 Click **Add** to add the logical devices that the sensor will manage.

The Adding page appears.

Figure 3-20 Adding Page



Step 3 In the Name field, enter the name of the logical device.

Step 4 In the Enable Password field, enter the enable password for the logical device (1 to 16 characters).

Note If there is no enable password, enter **none**.

Step 5 In the Password field, enter the Telnet or SSH password for the logical device (1 to 16 characters).

Note If there is no password, enter **none**.

Step 6 In the Username field, enter the username for the logical device.

Note If there is no username, enter **none**.

Note To reset the form, click **Reset**.

Step 7 Click **Apply to Sensor** to save your changes.

Configuring Blocking Devices

You can configure your sensor to block an attack by generating ACL rules for publication to a Cisco IOS router, or a Catalyst 6500 switch, or by generating shun rules on a PIX Firewall. The router, switch, or firewall is called a blocking device.

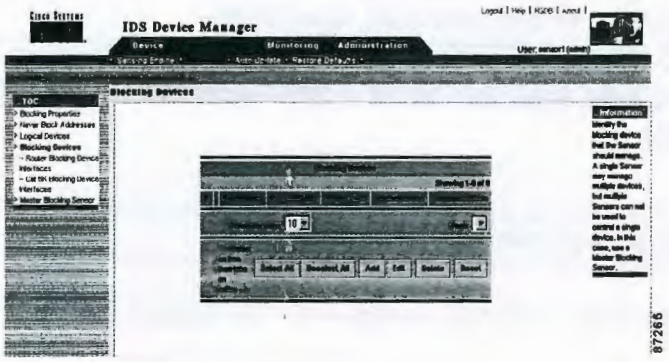
To configure blocking devices, follow these steps:

Step 1 Select **Configuration > Blocking Devices**.

The Blocking Devices page appears.

Caution A single sensor can manage multiple devices, but multiple sensors cannot be used to control a single device. In this case, use a master blocking sensor. See Configuring a Master Blocking Sensor, page 3-31, for more information.

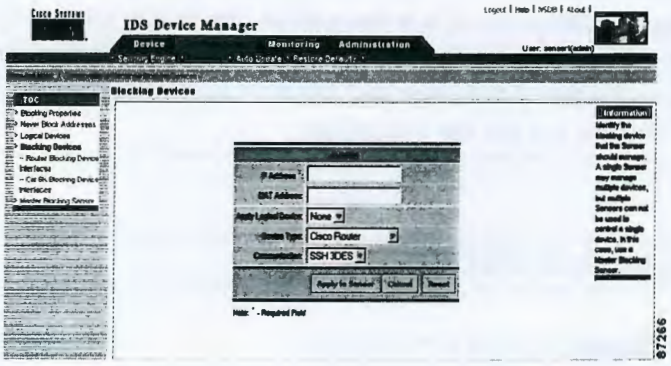
Figure 3-21 Blocking Devices Page



Step 2 Click **Add** to add a blocking device.

The Adding page appears.

Figure 3-22 Adding Page



Step 3 In the IP Address field, enter the IP address of the blocking device.

Step 4 In the NAT Address field, enter the NAT address of the blocking sensor.

Step 5 Select an option from the Apply Logical Device list box.

Note The same logical device can be used for multiple blocking devices. If you do not have logical devices set up, the only option is None.

Step 6 In the Device Type field, enter the type of device that will do the blocking:

- Cisco Router
- Catalyst 6000 VACL
- PIX Firewall

Step 7 In the Enable SSH field, select the type of secure communications you want to enable between the sensor and the blocking device:

- SSH 3DES
- SSH DES
- Telnet

Note Before you can use SSH 3DES or SSH DES, you have to use the **ssh host-key** *ipaddress* to obtain the public key in the correct format so that you can add the host to the known hosts list. Refer to the *Cisco Intrusion Detection System Appliance and Module Installation and Configuration Guide Version 4.0* for the procedure.

Note To reset the form, click **Reset**.

Step 8 Click **Apply to Sensor** to save your changes.

Configuring Router Blocking Device Interfaces

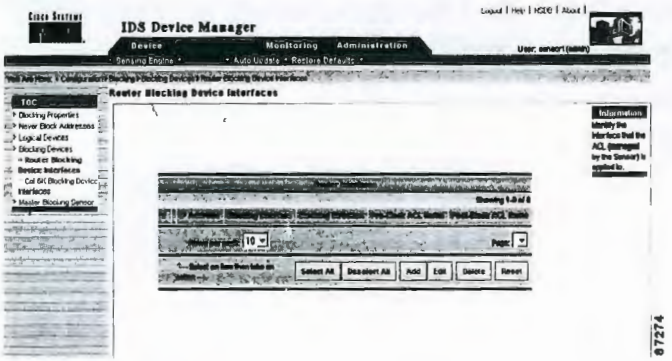
You must configure the blocking interfaces on the router and specify the direction of traffic you want blocked.

To configure the blocking interfaces on a router, follow these steps:

Step 1 Select **Configuration > Router Blocking Device Interfaces**.

The Router Blocking Device Interfaces page appears.

Figure 3-23 Router Blocking Device Interfaces Page



E C T
5216
- AC

Step 2 Click **Add** to configure the blocking interfaces on the router.

The Adding page appears.

Figure 3-24 Adding Panel

Step 3 In the IP Address field, enter the IP address of the router that will be used to block.

Step 4 In the Blocking Interface field, enter the interface on the router that will be used for blocking (1 to 32 characters).

Step 5 From the Blocking Direction list box, select the direction of the traffic through the interface that should be blocked (In, Out).

Step 6 In the Pre-Block ACL Name field, enter the name of the Pre-Block ACL (1 to 64 characters).

Step 7 In the Post-Block ACL Name field, enter the name of the Post-Block ACL (1 to 64 characters).

Note To reset the form, click **Reset**.

Step 8 Click **Apply to Sensor** to save your changes.

CPMI - CORREIOS
1329
Fls:
3701
Doc:

Configuring Catalyst 6K Blocking Device Interfaces

You must configure the blocking interfaces on the Catalyst switch and specify which VLAN you want blocked.

To configure the blocking interfaces on a Catalyst switch, follow these steps:

Step 1 Select **Configuration > CAT 6K Blocking Device Interfaces.**

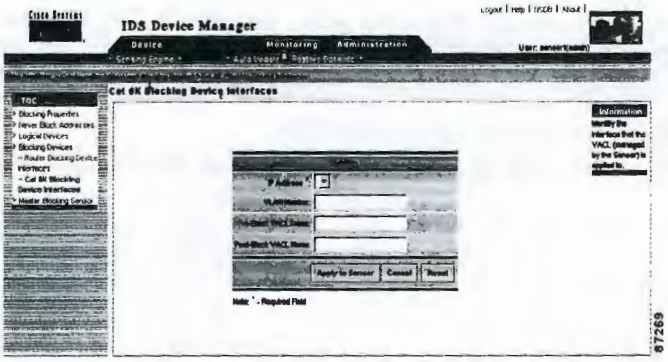
The CAT 6K Blocking Device Interfaces page appears.

Figure 3-25 CAT 6K Blocking Device Interfaces Page

Step 2 Click **Add** to configure the blocking interfaces on the router.

The Adding page appears.

Figure 3-26 Adding Page



E C T
5214
Paula
AC

Step 3 In the IP Address field, enter the IP address of the Catalyst switch that will be used to block.

Step 4 In the VLAN field, enter the VLAN number that the sensor will configure for blocking.

Step 5 In the Pre-Block VACL Name field, enter the name of the Pre-Block VACL (1 to 64 characters).

Step 6 In the Post-Block VACL Name field, enter the name of the Post-Block VACL (1 to 64 characters).

Note To reset the form, click **Reset**.

Step 7 Click **Apply to Sensor** to save your changes.

Configuring a Master Blocking Sensor

Multiple sensors can forward blocking requests to a specified master blocking sensor, which controls one or more devices. The sensor that is sending its block requests to the master blocking sensor is referred to as a "blocking forwarding sensor." On the blocking forwarding sensor, you must specify which remote host serves as the master blocking sensor; on the master blocking sensor you must add the blocking forwarding sensors to its remote host configuration.

Note Only the master blocking sensor is configured to manage the network devices. The blocking forwarding sensor should not be configured to manage network devices.

See Setting Up a Blocking Forwarding Sensors, page 3-33, for the procedure to configure the blocking forwarding sensor.

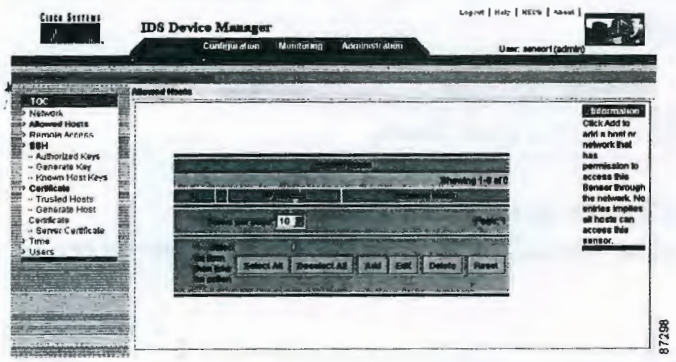
CPMI - CORREIOS
Fls: 1330
Doc: 3701

To configure blocking forwarding sensors to a master blocking sensor, follow these steps:

Step 1 Select **Device > Sensor Setup > Allowed Hosts**.

The Allowed Hosts page appears.

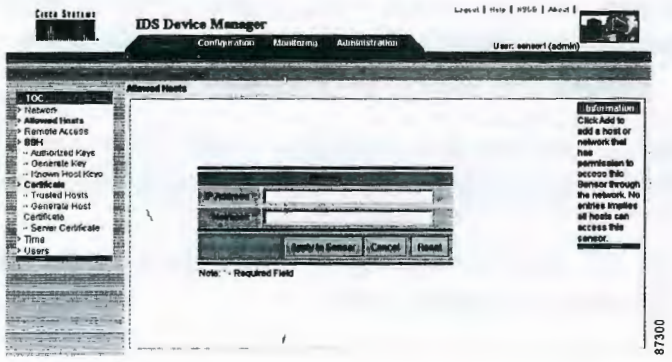
Figure 3-27 Allowed Hosts Page



Step 2 Click **Add** to add a sensor as a blocking forwarding sensor.

The Adding page appears.

Figure 3-28 Adding Page



Step 3 In the IP Addressfield, enter the IP address of the blocking forwarding sensor.

ECT 15212 Paula I L - AC

Step 4 If you are using SSH, the port number is the same port number that the master blocking sensor is using for IDM connections.

Note For example, if you are connecting using https, it is port 443 by default.

Step 5 In the User Name field, enter your IDS Device Manager administrator username.

Step 6 In the Password field, enter your IDS Device Manager administrator password.

Step 7 If you select Use SSH, you have to use the **tls trusted-host ip-address** *ipaddress* command.

Note To reset the form, click **Reset**.

Step 8 Click **Apply to Sensor** to save your changes.

Note Repeat this procedure for each sensor you want to identify as a blocking forwarding sensor.

Setting Up a Blocking Forwarding Sensors

The blocking forwarding sensor sends block requests to the master blocking sensor. On the blocking forwarding sensor, you must specify which remote host serves as the master blocking sensor.

See Configuring a Master Blocking Sensor, page 3-31, for more information on how to set up a master blocking sensor.

CPMI - C 3033
1331
Fls:
3701
Doc:

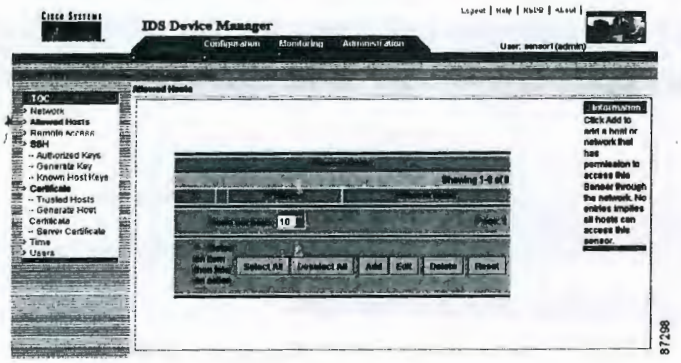
CPL - AC 5211 Paulo

To set up a blocking forwarding sensor, follow these steps:

Step 1 Select **Device > Sensor Setup > Allowed Hosts.**

The Allowed Hosts page appears.

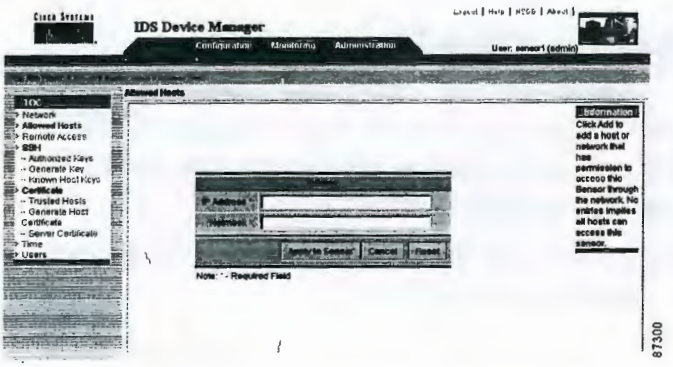
Figure 3-29 Allowed Hosts Page



Step 2 Click **Add** to add a sensor as a master blocking sensor.

The Adding page appears.

Figure 3-30 Adding Page



Step 3 In the IP Address field, enter the IP address of the master blocking sensor.

E C
5210
Paula
A C

Step 4 In the Netmask field, enter the netmask of the master blocking sensor.

Note To reset the form, click **Reset**.

Step 5 Click **Apply to Sensor** to save your changes.

The master blocking sensor is added to both the Allowed Hosts page and to the Master Blocking Sensor page.

Configuring Automatic Updates

You can configure automatic service pack and signature updates, so that when service pack and signature updates are loaded on a central FTP or SCP server, they will be downloaded and applied to your sensor. The timeout default is 5 minutes.

Note The sensor cannot automatically download service pack and signature updates from Cisco.com. You must download the service pack and signature updates from Cisco.com to your FTP or SCP server, and then configure the sensor to download them from the FTP or SCP server.

See Supported FTP Servers, page 3-37, for a list of supported servers.

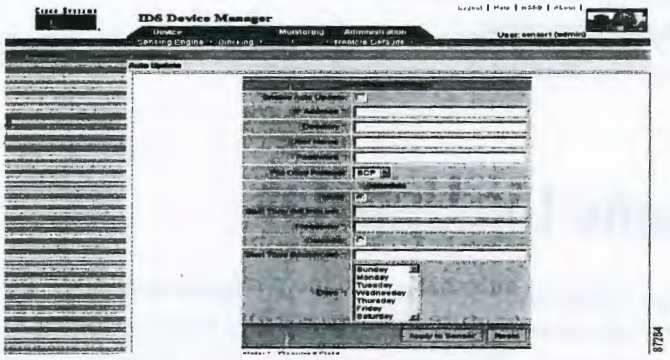
CPMI - CORREIOS
1332
Fls:
Doc: 3701

To configure automatic updates, follow these steps:

Step 1 Select **Configuration > Auto Update**.

The Auto Update page appears.

Figure 3-31 Auto Update Page



Step 2 Select the Enable Auto Update check box to enable automatic updates.

Step 3 In the IP Address field, enter the IP address of the server to poll for updates.

Step 4 In the Directory field, enter the path to the directory on the server where the updates are located (1 to 128 characters).

Step 5 In the Username field, enter the username to use when logging in to the server (1 to 16 characters).

Step 6 In the Password field, enter the username password on the server (1 to 16 characters).

Step 7 In the File Copy Protocol list box, select either **SCP** or **FTP**.

Step 8 For hourly updates, select **Hourly**, and follow these steps:

a. In the Start Time field, enter the time you want the updates to start (hh:mm:ss).

b. In the Frequency field, enter the hour interval at which you want every update to occur (1 to 8760).

For example, if you enter 5, every 5 hours the sensor looks at the directory of files on the server. If there is an available update candidate, it is downloaded and installed. Only one update is installed per cycle even if there are multiple available candidates.

ECT 5208 Rouda AC

Step 9 For calendar updates, select **Calendar**, and follow these steps:

a. In the Start Time field, enter the time you want the updates to start (hh:mm:ss).

b. In the Day field, select the day(s) you want to download updates.

Note To reset the form, click **Reset**.

Step 10 Click **Apply to Sensor** to save your changes.

Supported FTP Servers

The following FTP servers are supported for service pack and signature updates:

- Sambar FTP Server Version 5.0 (win32).
- Web-mail Microsoft FTP Service Version 5.0 (win32).
- Serv-U FTP-Server v2.5h for WinSock (win32).
- Solaris 2.8.
- HP-UX (HP-UX qdir-5 B.10.20 A 9000/715).
- Windows 2000 (Microsoft ftp server version 5.0).
- Windows NT 4.0 (Microsoft ftp server version 3.0).

Note The sensor cannot download service pack and signature updates from Cisco.com. You must download the service pack and signature updates from Cisco.com to your FTP server, and then configure the sensor to download them from your FTP server.

CPMI - CORREIOS
1333
Fls:
3701
Doc:

Restoring Default Settings

You can restore the default configuration to your sensor.

Warning **Clicking Apply to Sensor removes the current application settings and restores the default settings. Your network settings also return to the defaults and you immediately lose connection to IDS Device Manager and the CLI.**

To restore the default configuration, follow these steps:

Step 1 Select **Device > Configuration > Restore Defaults**.

The Restore Defaults page appears.

Figure 3-32 Restore Defaults Page

Step 2 Click **Apply to Sensor** to restore the default configuration.

The IP address, netmask, default gateway, allowed hosts, password, and time will not be reset. Manual and automatic blocks also remain in effect.

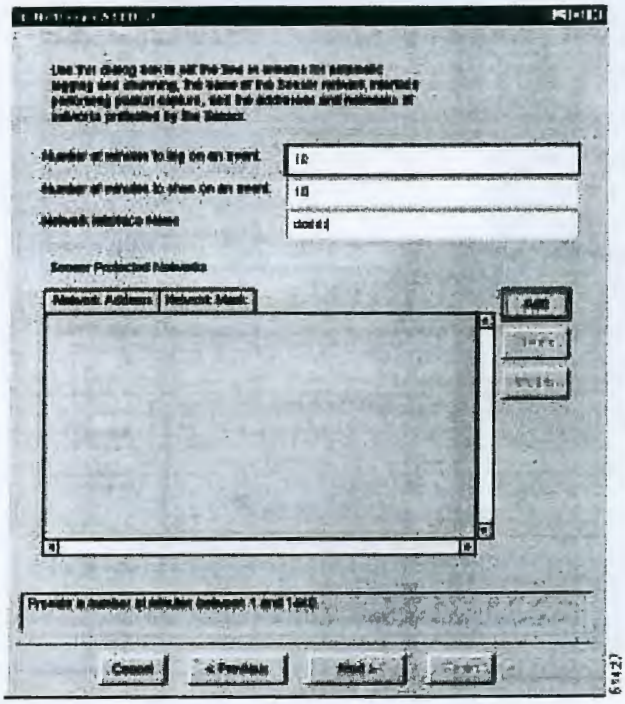
Apêndice DA

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1334
Doc: 3701

Doc: 3701
Fls: 1335
CPMI - CORREIOS
ROS Nº 03/2005 - CN

E
5200
Paula
CPL - AC

Figure 6-4 Configuring the Sensor

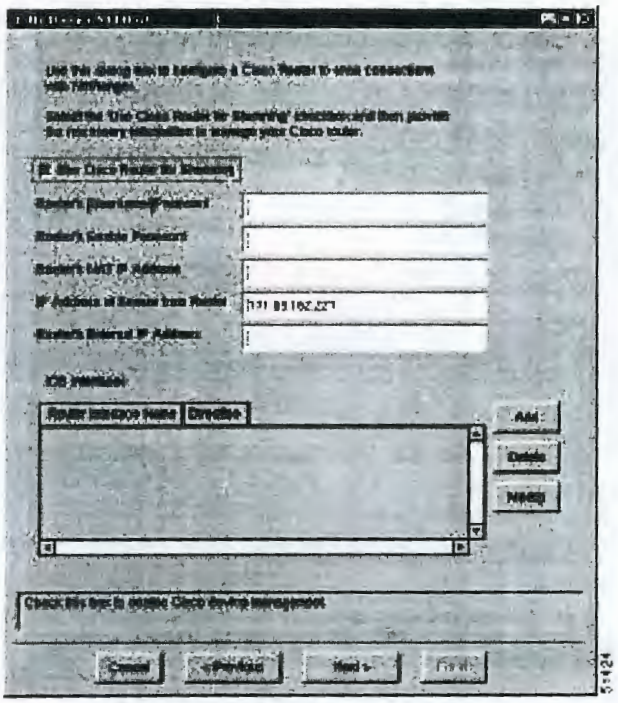


Step 9 If you want to configure a Cisco router to shun connections with the Director, select the **Use Cisco Router for Shunning** check box, fill in the rest of the router information, and click **Finish** (see Figure 6-5).

Note This option is not available for the IDSM.

E C T
15199
Paula
C P L - A C

Figure 6-5 Configuring a Cisco Router for Shunning



The host definition is complete.

Doc: 3701
Fls: 1336
ROS Nº 03/2005 - CN
CPMI - CORREIOS

E C T
5196
Paula
A C I

Step 11 Click **OK** to close the **Communications** dialog box.

Step 12 To apply the configuration changes, click the newly created transient version on the **Configuration Versions** window and click **Apply**.

Note Clicking **Cancel** discards any configuration changes.

Configuring Data Management

Note The following section applies to only the version 2.5 Sensor.

IDS data management is handled by a daemon called *sapd*. *sapd* collects log files created in the /usr/nr/var directory by another daemon called *loggerd*. The rate at which *sapd* collects log files (which can be either ASCII event logs or binary IP logs), is controlled by user-configurable thresholds.

The main goals of data management are:

- Collection of data in a fast, fault-tolerant manner
- Staging of that data to industrial-strength relational database management systems or archives.
- Preventing disk systems from filling up

This section includes the following topics:

- Setting Data Collection and Staging
- Setting Triggers
- Setting File Management Viewing Mode

ECT 3195 Paula CPL

Setting Data Collection and Staging

To configure data collection and staging, follow these steps:

Step 1 On the Director interface (NetRanger submap), click the machine icon you want to configure.

Step 2 Click **Security>Configure**.

The **Configuration Versions** window opens.

Step 3 In the currently applied version (in bold), double-click **Data Management**.

The **Data Management** dialog box opens.

Step 4 Click the **Logging** tab.

Step 5 Set the maximum log file size (in bytes) in the **bytes** field.

The default log file size is **300,000** bytes.

Step 6 Set the maximum log file age (in minutes) in the **minutes** field.

The default log file age is **240** minutes.

Note The log file size and log file age both control how fast *sapd* pulls the files from /usr/nr/var. For example, if you set the maximum log file size to 100 kilobytes, and set the maximum age to 30 minutes, then *sapd* pulls the log file in (a) 30 minutes if its file size is less than 100 kilobytes, or (b) sooner, if the file size reaches 100 kilobytes before the 30 minute threshold.

Step 7 Set an alarm's minimum context level (in other words, alarms below a certain severity will not have context data stored in the logfile) in the **Minimum context Level** field.

The default minimum context level is **2**.

Step 8 Click the **Database** tab.

Doc: 3701
Fls: 1337
ROS Nº 03/2005 - CN
CPMI - CORREIOS

ECT
1 5194
Paula
CPL - AC

Step 9 Set up a database account by editing the **User** and **Password** fields for User 1.

Note **User 2** and **Auxiliary 1** through **Auxiliary 3** are normally only used when installing a Remedy ARS Trouble Ticketing System (see "Setting Up a Remedy ARS Trouble Ticketing System" section in Appendix A, "Installing Third-Party RDBMS Tools," for more information).

Step 10 Click **OK** to close the **Data Management** dialog box.

Step 11 To apply the configuration changes, click the newly created transient version on the **Configuration Versions** window and click **Apply**.

Note Clicking **Cancel** discards any configuration changes.

Setting Triggers

The *sapd* daemon bases all its actions on triggers. Each trigger consists of a condition and an action. The condition defines when to launch an action.

To create a sample trigger, follow these steps:

Step 1 On the Director interface (NetRanger submap), click the machine icon you want to configure.

Step 2 Click **Security>Configure**.

The **Configuration Versions** window opens.

Step 3 In the currently applied version (in bold), double-click **Data Management**.

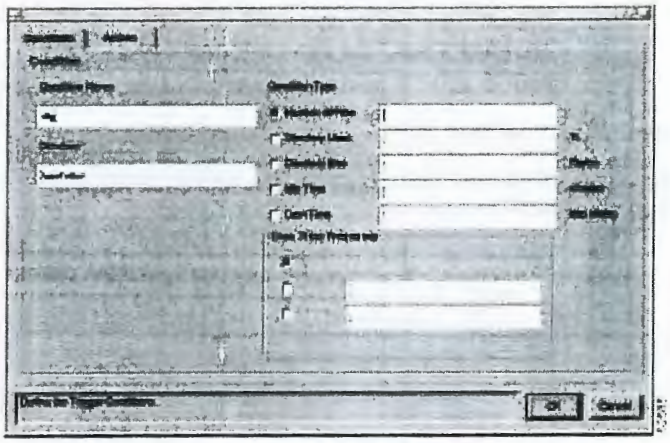
The **Data Management** dialog box opens.

Step 4 Click the **Triggers** tab.

Step 5 Click **Add**.

The **Add New Trigger** dialog box opens (see Figure 6-6).

Figure 6-6 Add New Trigger Dialog Box



Step 6 Type the name of your condition in the **Condition Name** box.

Step 7 Type `/usr/nr/bin` in the **Condition Directory** box.

Step 8 Select the **Number of Files** check box and type `5` in the field next to the check box.

Step 9 Select the **Notify** check box.

Step 10 Click **OK** to close the **Add New Trigger** dialog box.

Doc: 3701
Fls: 1338
CPMI - CORREIOS
RQS Nº 03/2005 - CN

ECT - AC
5192
Paula

Step 11 Click the **Notification** tab.

Step 12 Type a valid e-mail address in the **Notify Person #1** box.

The Director sends notifications to this e-mail address when the number of files in /usr/nr/bin reaches 5.

Step 13 Edit the **Notify Interval** field to change the minimum time between notifications.

The default interval is **60** minutes.

Step 14 Click **OK** to close the **Data Management** dialog box.

Step 15 To apply the configuration changes, click the newly created transient version on the **Configuration Versions** window and click **Apply**.

Note Clicking **Cancel** discards any configuration changes.

Setting File Management Viewing Mode

To set file management viewing mode, follow these steps:

Step 1 On the Director interface (NetRanger submap), click the Director icon.

Step 2 Click **Security>Configure**.

The **Configuration Versions** window opens.

Step 3 Right-click the currently applied version (in bold) and click **Open Folder** (or double-click the version to expand it).

Step 4 Right-click **Data Management** and click **Open**.

The **Data Management** dialog box opens.

Step 5 Click the **General** tab.

Step 6 The default setting is verbose mode. To change the viewing preference to brief, make sure that **Verbose DMP Display** is *not* selected.

Step 7 Click **OK** to close the **Data Management** dialog box.

Step 8 On the **Configuration Versions** window, click the transient folder and click **Apply**.

Step 9 After you set your file management viewing mode, click **Security>Show>Database Info** to display the following information:

- Overall status
- Trigger history and configuration
- Action Configuration
- Directory summary for /usr/nr/var

Configuring Device Management and Shunning

Device management refers to the Sensor's ability to dynamically reconfigure the filters and access control lists on a router to shun an attacker. This functionality is provided by the *managed* daemon. *Shunning* refers to the Sensor's ability to use a network device to deny entry to a specific network host or an entire network.

This section describes the three major tasks involved with using a router to shun an attacker, and includes the following topics:

- Setting Up Device Management
- Setting Up Shunning
- Setting Up Intrusion Detection

Doc: 3701
Fls: 1339
CPMI - CORREIOS
ROS Nº 05/2005 - CN

ECT
15190
Paula
CPL - AC

Setting Up Device Management

To configure device management, follow these steps:

Step 1 On the Director interface (NetRanger submap), click the machine icon you want to configure.

Step 2 Click **Security>Configure**.

The **Configuration Versions** window opens.

Step 3 In the currently applied version (in bold), double-click **Device Management**.

The **Device Management** dialog box opens.

Step 4 Click the **Devices** tab.

Step 5 Click **Add** to add a router to *managed*'s list of network devices.

Enter the following information about the router in the following fields:

- **IP Address**
- **Device Name**
- **Username/Password**
- **Enable Password**
- **NAT IP Address**

Note You must also ensure that the Telnet service is enabled on managed routers. Refer to your router's documentation for more information.

Step 6 Click the **Interfaces** tab.

Step 7 Click **Add**.

ECT 5189 Paula IAC

Step 8 Enter the following information for each interface on the managed network device:

- **IP Address**—The IP address assigned to the router interface.
- **Interface Name**—The name of the router interface (for example, "ethernet0").
- **Direction**—The direction of the network traffic passing through the interface.

Step 9 Click **OK** to close the **Device Management** dialog box.

Step 10 To apply the configuration changes, click the newly created transient version on the **Configuration Versions** window and click **Apply**.

Note Clicking **Cancel** discards any configuration changes.

Setting Up Shunning

After you set up device management, you need to set up shunning.

This section includes the following topics:

- Sensor Already Configured to Use Cisco Router for Shunning
- Configuring a Sensor to Use Cisco Router for Shunning

Doc: 3701
Fls: 1340
CPMI - CORREIOS
ROS Nº 03/2005 - CN

ECT 5188 Paula CPL - AC

Sensor Already Configured to Use Cisco Router for Shunning

If during the final Sensor configuration, you selected **Use Cisco Router for Shunning** on the **Cisco Router Information** window of the **Add Host** dialog box (see "Adding a Host"), then the Sensor's shunning infrastructure is in place, and all you need to do is add specific information:

Step 1 On the Director interface (NetRanger submap), click the machine icon you want to configure.

Step 2 Click **Security>Configure**.

The **Configuration Versions** window opens.

Step 3 In the currently applied version (in bold), double-click **Device Management**.

The **Device Management** dialog box opens.

Step 4 Click the **Shunning** tab.

Step 5 Under **Addresses Never to Shun**, click **Add** to add entries for the local Director, Sensor, and router, at the very minimum.

Step 6 Under **Shunning Servers**, add an entry for the Sensor that will perform shunning.

Step 7 Click **OK** to close the **Device Management** dialog box.

Step 8 To apply the configuration changes, click the newly created transient version on the **Configuration Versions** window and click **Apply**.

Note Clicking **Cancel** discards any configuration changes.

Configuring a Sensor to Use Cisco Router for Shunning

If during the final Sensor configuration, you selected *not* to use a Cisco router for shunning, you need to check whether *managed* is enabled on the Sensor before setting up shunning:

Step 1 On the Director interface (NetRanger submap), click the machine icon you want to configure.

Step 2 Click **Security>Configure**.

The **Configuration Versions** window opens.

Step 3 In the currently applied version (in bold), double-click **Daemons**.

The **Daemons** dialog box opens.

Step 4 Make sure that *managed* is set to **Yes** in the table and click **OK** to close the **Daemons** dialog box.

Step 5 Follow the procedure in "Sensor Already Configured to Use Cisco Router for Shunning" to complete the shunning configuration.

Doc:
Fls: 3701
1341
ROS N° 03/2005 - CN
CPMI - CORREIOS

ECT
5186
Paula
CPI - AC

Configuring Policy Violation Logging

This section describes the following topics:

- Policy Violation Logging in the IDS
- Configuring and Monitoring User-Defined ACLs
- Configuring and Monitoring IDS-Defined ACLs

Policy Violation Logging in the IDS

The router's *syslogd* daemon can be configured to send information to a Sensor regarding denied network traffic. The Sensor can then forward this data to the Director, which can then display a policy violation alarm.

Note The Director accepts ACL policy violations from routers running Cisco IOS Release 10.3 and higher.

There are two kinds of ACLs that can be configured to work with the Director:

- User-defined ACLs, which are created and updated by users.
- IDS-defined ACLs, which are created and updated by the *managed* daemon.

This section includes the following topics:

- Configuring and Monitoring User-Defined ACLs
- Configuring and Monitoring IDS-Defined ACLs

Configuring and Monitoring User-Defined ACLs

There are three procedure to follow for configuring and monitoring user-defined ACLs. This section includes the following topics:

- Manually Configuring the Router to Communicate with the Sensor
- Manually Configuring the ACLs to Log Policy Violations
- Configuring the Sensor to Accept syslogd Traffic From the Router

Manually Configuring the Router to Communicate with the Sensor

To manually configure the router to communicate with the Sensor, follow these steps:

Step 1 Log on to the router and enter enable mode by typing `en` and the enable password.

Step 2 Enter configuration mode by typing:

```
conf t
```

Step 3 Type the following commands:

```
logging sensor_ip_address
logging trap info
```

where *sensor_ip_address* is the IP address of the Sensor's command and control interface.

Step 4 Exit configuration mode by pressing Ctrl-Z.

Step 5 To make the changes permanent on the router, type:

```
wr mem
```

Doc:
Fls: 3701
1342
CPMI - CORREIOS
ROS Nº 03/2005 - CN

ECT
5184
Paula
CPL - AC

Manually Configuring the ACLs to Log Policy Violations

To manually configure the ACLs to log policy violations, follow these steps:

Step 1 Set the user-defined ACLs on each router to send policy violation information by adding the text string "log" to the end of each line that defines a deny rule. For example:

```
access-list 199 deny tcp host 10.1.1.1 any log
```

This rule denies TCP traffic between host 10.1.1.1 and "any" other host. The string "log" at the end of the deny rule ensures that the policy violation is logged.

Note All rules not containing the text string "log" at the end of the line will cause the router to not log the policy violation.

Step 2 To make the changes permanent on the router, type:

```
wr mem
```

Configuring the Sensor to Accept *syslogd* Traffic From the Router

To configure the Sensor to accept syslogd traffic from the router, follow these steps:

Step 1 On the Director interface (NetRanger submap), click the Sensor icon.

Step 2 Click **Security>Configure**.

The **Configuration Versions** window opens.

Step 3 In the currently applied version (in bold), double-click **Intrusion Detection**.

The **Intrusion Detection** dialog box opens.

Step 4 Click the **Data Sources** tab.

Step 5 In the **Data Sources** field, make sure that the IP address and netmask of the router sending the syslog information is present.

ECT 5183 Paula CPL AC

Step 6 If this information is not present, click **Add** and then type the IP address and subnet mask in the appropriate fields.

Step 7 Click the **Profile** tab.

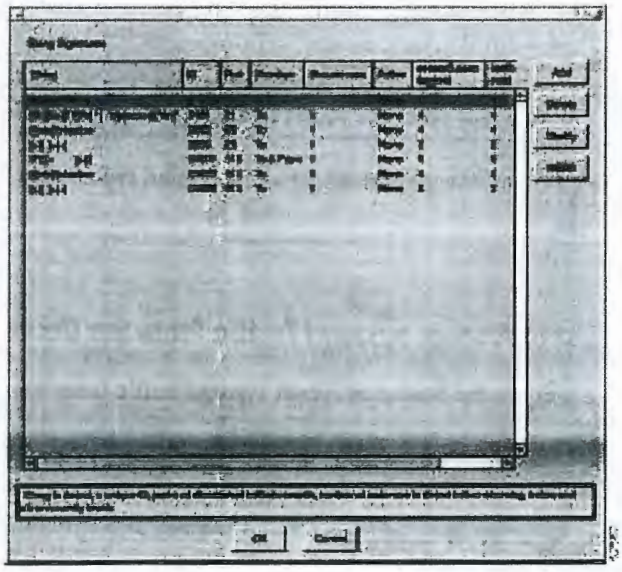
Step 8 Make sure that **Setup Method** is set to **Manual Configuration**.

Step 9 Click **Modify Signature**.

Step 10 Scroll down to the **Security Violations** signature and click **Expand**.

The **Policy Violations** dialog box opens (Figure 6-7).

Figure 6-7 Policy Violations Dialog Box



Step 11 Click **Add** to add the name of the Cisco ACL that sends syslog data to the Sensor.

Step 12 Choose an action from the list in response to the policy violation alarm, and enter the alarm's severity level for each destination.

Step 13 Repeat Steps 11 and 12 for each ACL added.

Step 14 Click **OK** to close the **Policy Violations** dialog box.

Step 15 Click **OK** to close the **Signatures** dialog box.

Doc:
3701
Fls:
1343
CPMI - CORREIOS
RGS Nº 03/2005 - CN

5182
Paulo

Step 16 Click **OK** to close the **Intrusion Detection** dialog box.

Step 17 To apply the configuration changes, click the newly created transient version on the **Configuration Versions** window and click **Apply**.

Note Clicking **Cancel** discards any configuration changes.

Configuring and Monitoring IDS-Defined ACLs

Configuring IDS-defined ACLs is similar to configuring user-defined ACLs, except that you can use the Director's utilities to ease setup and monitoring. Also, IDS-defined ACLs are created and updated by the *managed* daemon.

There are three procedures to follow to configure and monitor IDS-defined ACLs. This section includes the following topics:

- Configuring the Router to Communicate with the Sensor
- Configuring the IDS-Defined ACLs to Log Policy Violations
- Configuring the Sensor to Accept syslog Traffic from the Router

Configuring the Router to Communicate with the Sensor

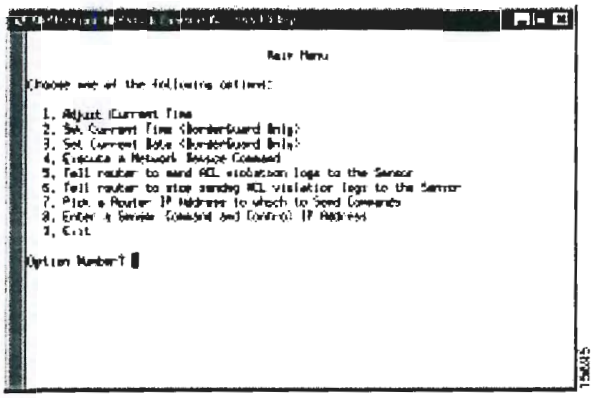
To configure the router to communicate with the Sensor, follow these steps:

Step 1 On the Director interface (NetRanger submap), click the Sensor icon that is to receive the policy violation information from the router.

Step 2 Click **Security>Network Device**.

The **Network Device Utility** window opens. (see Figure 6-8)

Figure 6-8 Network Device Utility Window



Step 3 To command the router to send policy violation information to the Sensor, choose option **5**.

Step 4 When prompted, type the Sensor's IP address, and type `y` to confirm.

Step 5 Read the information and press Enter when prompted.

Step 6 Choose option **9** to exit the **Network Device Utility**.

Doc: 3701
Fls: 1344
CPMI - CORREIOS
RGS Nº 03/2005 - CN

ECT 5180 Paula CPL - AC

Configuring the IDS-Defined ACLs to Log Policy Violations

You can configure the IDS-defined ACLs to log policy violations temporarily or permanently;

This section includes the following topics:

- Temporary Policy Violation Logging
- Permanent Policy Violation Logging

Temporary Policy Violation Logging

To configure the IDS-defined ACLs to log policy violations temporarily, follow these steps:

Step 1 On the Director interface (NetRanger submap), click the Sensor icon that is to receive the policy violations from the router.

Step 2 Click **Security>Advanced>ACL Syslogs>Enable**.

Note To disable ACL logging, click **Security>Advanced>ACL Syslogs>Disable**.

Permanent Policy Violation Logging

To configure the IDS-defined ACLs to log policy violations even after the Sensor restarts/reboots, follow these steps:

Step 1 On the Director interface (NetRanger submap), click the Sensor icon that is to receive the policy violations from the router.

Step 2 Click **Security>Configure**.

The **Configuration Versions** window opens.

Step 3 In the currently applied version (in bold), double-click **Device Management**.

The **Device Management** dialog box opens.

Step 4 Click the **General** tab.

ECT 5179 Pacific CBL AC

Step 5 Click **Enable ACL Logging**.

Step 6 Click **OK**.

Step 7 To apply the configuration changes, click the newly created transient version on the **Configuration Version** window and click **Apply**.

Note Clicking **Cancel** discards any configuration changes.

Configuring the Sensor to Accept syslog Traffic from the Router

To configure the Sensor to accept syslogd traffic from the router, follow these steps:

Step 1 On the Director interface (NetRanger submap), click the Sensor icon that is to receive the policy violations from the router.

Step 2 Click **Security>Configure**.

The **Configuration Versions** window opens.

Step 3 In the currently applied version (in bold), double-click **Device Management**.

The **Device Management** dialog box opens.

Step 4 Click the **Shunning** tab.

Step 5 Make note of the entry under **Cisco ACL Number** (for example, the entry might be "199").

Step 6 Click **OK**.

Step 7 In the newly created version folder in the **Configuration Versions** window, double-click **Intrusion Detection**.

The **Intrusion Detection** dialog box opens.

Step 8 Click the **Data Sources** tab.

Step 9 Under **Data Sources**, ensure that the IP address and netmask of the router sending the syslog information is present.

Step 10 If this information is not present, click **Add** and then type the IP address and subnet mask in the appropriate fields.

Doc: 3701
Fls: 1345
CPMI - CORREIOS
ROS Nº 09/2005 - CN

ECT 5178 Paula CPL - AC

Step 11 Click the **Profile** tab.

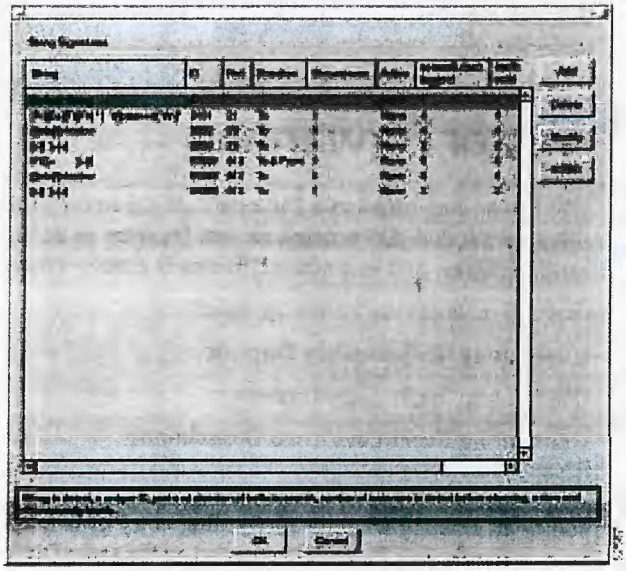
Step 12 Ensure that **Setup Method** is set to **Manual Configuration**.

Step 13 Click **Modify Signatures**.

Step 14 Scroll down to the **Security Violations** signature and click **Expand**.

The **Policy Violations** dialog box opens (Figure 6-9).

Figure 6-9 Policy Violations Dialog Box



Step 15 Click **Add** to add the number of the Cisco ACL from Step 5.

Step 16 Choose an action from the list in response to the policy violation alarm, and enter the alarm's severity level for each destination.

Step 17 Click **Add** to add an ACL whose number is one less than the ACL added in Step 15.

Step 18 When the Director dynamically changes an ACL in response to network activity, it alternates between the two ACLs when applying them.

Step 19 Repeat Steps 15 through 17 for each ACL added.

Step 20 Click **OK** to close the **Policy Violations** dialog box.

Step 21 Click **OK** to close the **Signatures** dialog box.

Step 22 Click **OK** to close the **Intrusion Detection** dialog box.

Step 23 To apply the configuration changes, click the newly created transient version on the **Configuration Versions** window and click **Apply**.

Note Clicking **Cancel** discards any configuration changes.

Configuring Director Forwarding

Director forwarding refers to a Director's ability to forward all errors and alarms it receives to another IDS process on that Director or another Director. Forwarding alarms to a secondary Director is a three-phase task.

This section includes the following topics:

- Configuring the Secondary Director
- Configuring the Primary Director
- Configuring Event Levels and Destinations

Note To modify an existing Director forwarding entry or to add an entry to Director forwarding for an IDS daemon on the same Director, then proceed directly to the "Configuring Event Levels and Destinations" section.

Doc: 3701
Fls: 1346
CPMI - CORREIOS
RGS Nº 03/2005 - CN

ECT 5176 Pauba

Configuring the Secondary Director

The first phase of configuring Director forwarding is to give the secondary Director (the one receiving the forwarded information) information about the primary Director (the one that is forwarding information).

Step 1 On the *secondary Director's* interface (NetRanger submap), click the secondary Director icon.

Step 2 Click **Security>Configure**.

The **Configuration Versions** window opens.

Step 3 Double-click **System Files**.

Step 4 Double-click **Organizations**.

Step 5 If the primary Director is in a different organization than the secondary Director, add the primary Director's organization name and click **OK**.

Step 6 Double-click **Hosts**.

Step 7 Add the primary Director's host name and click **OK**.

Step 8 Double-click **Routes**.

Step 9 Add the following information about the primary Director:

- Host name
- Connection number
- IP address of host

ECT 5175 Paula CPL - AC

- UDP port number used for communication
- A reserved Type column, which should always have **1** as an entry
- Heartbeat

Note The heartbeat is a time interval, in seconds, that *postofficed* uses when transmitting route verification messages. If the heartbeat is set to 5, then *postofficed* waits 5 seconds before transmitting another heartbeat. Furthermore, *postofficed* waits a period of time equal to three times the heartbeat interval for a response. If a response does not return in time, then *postofficed* assumes the route is down and sends an error alarm to the Director.

Step 10 Click **OK**.

Step 11 Double-click **Authorizations**.

Step 12 Make sure that the primary Director has the following permissions at a minimum:

- Get
- Getbulk

Step 13 Click **OK**.

Step 14 To apply the configuration changes, click the newly created transient version on the **Configuration Versions** window and click **Apply**.

Note Clicking **Cancel** discards any configuration changes.

Doc: 3701
Fls: 1347
CPMI - CORREIOS
RGS Nº 03/2005 - CN

ECT 5174 Paula CL-AC

Configuring the Primary Director

The second phase in setting up Director forwarding is to instruct the primary Director to forward information to the secondary Director.

Step 1 On the primary Director's interface (NetRanger submap) click **Security>Configure**.

The **NetRanger Configuration File Management Utility** (nrConfigure) window opens.

Step 2 Click **File>Add Host**.

The **NetRanger Add Host** wizard opens.

Step 3 Read the instructions on the first window of the **Add Host** wizard and click **Next**.

Step 4 Select the organization name to which the secondary Director belongs. If you need to, click **Create** to add an entry for the secondary Director's organization.

Step 5 Type the *secondary Director's* host name, host ID, and host IP address in the appropriate fields.

Step 6 Click **Next**.

The **Host Type** window opens.

Step 7 Select **Forward alarms to secondary Director**.

Step 8 Click **Next**.

Step 9 Click **Finish**.

Configuring Event Levels and Destinations

The final phase of setting up Director forwarding is to configure event levels and daemons receiving the forwarded information. By default, the primary Director forwards all alarm levels to the secondary Director's *smid* daemon.

If you want to change these default settings, or add a new IDS service to which events should be forwarded, do the following:

Step 1 On the *primary Director's* interface, click the *primary Director* icon.

Step 2 Click **Security>Configure**.

The **Configuration Versions** window opens.

Step 3 In the currently applied version (in bold), double-click **Director Forwarding**.

The **Director Forwarding** dialog box opens.

Step 4 Click the **Forwarding** tab.

An entry should exist for *loggerd* for the primary Director. If alarms are being forwarded to a secondary Director, an entry should also exist for *smid* for the secondary Director.

Step 5 To add an IDS daemon to the list of entries, click **Add**. To change an existing entry, select the entry and click **Modify**.

Enter the following information about each daemon:

- **Host**—Select the Director's host name from the drop-down list.
- **Service**—Select the Director daemon to which you want data forwarded.

  Select *loggerd* if you want the Director to receive a duplicate copy of a Sensor's log files. Select *smid* if you want the primary Director to receive duplicate alarms generated by the Sensor to a secondary Director.
- **Minimum Level**—Type the minimum alarm level for alarm data sent to the Director.
- **Commands**—Select **Yes** if you want commands sent to the daemon. Otherwise, select **No**.

Doc: 3701
Fls: 1348
CPMI - CORREIOS
RQS Nº 03/2005 - CN

5172
Paula

- **Errors**—Select **Yes** if you want errors sent to the daemon. Otherwise, select **No**.
- **Alarms**—Select **Yes** if you want alarms sent to the daemon. Otherwise, select **No**.
- **IP Logs**—Select **Yes** if you IP logs sent to the daemon. Otherwise, select **No**.

Step 6 Click **OK** to close the **Director Forwarding** dialog box.

Step 7 To apply the configuration changes, click the newly created transient version on the **Configuration Versions** window and click **Apply**.

Note Clicking **Cancel** discards any configuration changes.

Configuring Event Processing

Event processing is managed by the *eventd* daemon. *eventd* processes alarms sent to it and executes user-defined actions. It is generally intended to accommodate batch or background processes, such as e-mail notification, SNMP trap generation, or other user-defined processes.

This section provides information on setting up basic event processing, and includes the following topics:

- Configuring and Enabling eventd
- Configuring an Event Source to Send Events to eventd

Note For additional details on setting up e-mail notification, SNMP trap generation, or running custom scripts under *eventd*, refer to "Advanced Event Processing Support" in Chapter 9, "Advanced Director Functions."

Configuring and Enabling *eventd*

To configure the event processing infrastructure, follow these steps:

Step 1 On the Director interface (NetRanger submap), click the machine icon whose *eventd* process you want to enable.

Step 2 Click **Security>Configure**.

The **Configuration Versions** window opens.

Step 3 In the currently applied version (in bold), double-click **Event Processing**.

The **Event Processing** dialog box opens.

Step 4 Click the **Applications** tab.

Step 5 Click **Add** to add rows to the listing, and click **Delete** to delete rows from the listing.

Each row has three columns:

- **Script ID**—The ID number is autogenerated by nrConfigure.
- **Severity Level**—Type an alarm severity level here. *eventd* executes the script you specify for each event whose severity level is **greater than or equal** to this severity level, provided that the events meet the timing thresholds that you set (see Step 6).
- **Script Name**—Type the full path and name of the script you want to execute (for example, `/usr/nr/myscript`). If you want to set up e-mail notification, type `/usr/nr/bin/eventd/event` in this field. To generate SNMP traps, type `/usr/nr/bin/nrSnmpTrap` in this field.

Note For additional details on setting up e-mail notification, SNMP trap generation, or running custom scripts under *eventd*, refer to "Advanced Event Processing Support" in Chapter 9, "Advanced Director Functions."

Step 6 Click the **Timing** tab.

This tab controls how often *eventd* executes an action when an event is received.

Doc:
Fls: 3701
1349
ROS Nº 03/2005 - CN
CPMI - CORREIOS

ECT
5170
Paula
CPL - AC

Step 7 Type the following information in the appropriate fields:

- **Consolidation Interval(s)**—The number of seconds in the interval during which *eventd* collects events.
- **Alarm Count Thresholds**—The number of events that must be received in the specified interval to force the execution of an action. This field can contain one or more integer values separated by commas or spaces.

  For example, an entry of "1, 5, 100" would execute an action the first, fifth, and hundredth time an event occurred during the specified interval.

Step 8 Click **OK** to close the **Event Processing** dialog box.

Step 9 On the current transient version of code, double-click **Daemons**.

The **Daemons** dialog box opens.

Step 10 Enable **nr.eventd** by changing its status to **Yes**.

Step 11 Click **OK** to close the **Daemons** dialog box.

Step 12 To apply the configuration changes, click the newly created transient version on the **Configuration Versions** window and click **Apply**.

Note Clicking **Cancel** discards any configuration changes.

Configuring an Event Source to Send Events to *eventd*

After configuring and enabling eventd, you must tell an event source (a Sensor or Director) to send notifications to eventd. The procedure for configuring Sensors and Directors differs.

This section includes the following topics:

- Configuring a Sensor to Send Events to eventd
- Configuring a Director to Send Events to eventd

ECT 5169 Faura CPL AC

Configuring a Sensor to Send Events to eventd

To configure a Sensor to send event notifications to eventd, follow these steps:

Step 1 On the Director interface (NetRanger submap), click a Director icon.

Step 2 Click **Security>Configure**.

The **Configuration Versions** window opens.

Step 3 Double-click **Destinations** under the currently applied version (in bold).

The **Destinations** dialog box opens.

Step 4 Click **Add**.

Step 5 Add the following information in each of the fields:

- **Host**—Type the Sensor's host name.
- **Application**—Type `eventd`.
- **Severity Level**—Type a minimum severity level to send.

  Note This number should match the *lowest* severity entered in the **Applications** tab of the **Event Processing** dialog box.

- **Event Type**—Choose either **IP Logs**, **Errors**, **Commands**, or **Alarms** from the field's drop-down menu.

Step 6 Click **OK** to close the **Destinations** dialog box.

Step 7 To apply the configuration changes, click the newly created transient version on the **Configuration Versions** window and click **Apply**.

Note Clicking **Cancel** discards any configuration changes.

ECT 5168 Paula CPL - AC

Configuring a Director to Send Events to eventd

To configure a Director to send event notifications to eventd, follow these steps:

Step 1 On the Director interface (NetRanger submap), click a Director icon.

Step 2 Click **Security>Configure**.

The **Configuration Versions** window opens.

Step 3 Double-click **Director Forwarding** under the currently applied version (in bold).

The **Director Forwarding** dialog box opens.

Step 4 Click the **Forwarding** tab. (An entry should exist for the primary Director.)

Step 5 Click **Add**.

Step 6 Enter the following information about each Director:

- **Host**—Select the Director's host name from the drop-down list.
- **Service**—Select *eventd*.
- **Minimum Level**—Type a minimum severity level to send.

Note This number should match the **lowest** severity entered in the Applications tab of the **Event Processing** dialog box.

- **Commands**—Select **Yes** if you want commands sent to the Director. Otherwise, select **No**.
- **Errors**—Select **Yes** if you want errors sent to the Director. Otherwise, select **No**.
- **Alarms**—Select **Yes** if you want alarms sent to the Director. Otherwise, select **No**.

Step 7 **IP Logs**—Select **Yes** if you want IP logs sent to the Director. Otherwise, select **No**.

Step 8 Click **OK** to close the **Director Forwarding** dialog box.

Step 9 To apply the configuration changes, click the newly created transient version on the **Configuration Versions** window and click **Apply**.

Note Clicking **Cancel** discards any configuration changes.

Configuring Intrusion Detection

This section describes the following topics:

- Intrusion Detection in the Director
- Setting Up Intrusion Detection
- Advanced Intrusion Detection Settings

Intrusion Detection in the Director

Intrusion Detection is handled by the *packetd* and *sensord* daemons. *packetd* normally operates from a Sensor working in standalone mode (in other words, without a packet filter). *sensord* normally operates on a Sensor working with a packet filter that is forwarding copies of network packets to it.

Doc: 3791
Fls: 1351
CPMI - CORREIOS
RGS Nº 03/2005 - CN

ECT 5166 Paula CPL - AC

Setting Up Intrusion Detection

You have two choices for setting up intrusion detection on a Sensor:

- You can use a *profile-based configuration*, which allows you to use pre-defined profiles for intrusion detection. Using profiles allows for both a fast configuration and fast integration of new signatures during software upgrades.
- You can use a *manual configuration*, which allows you to configure individual signatures, giving you control over almost every aspect of intrusion detection on a Sensor.

This section includes the following topics:

- Setting Up a Profile-Based Configuration
- Setting Up a Manual Configuration

Setting Up a Profile-Based Configuration

To set up a profile-based configuration, follow these steps:

Step 1 On the Director interface (NetRanger submap), click the Sensor icon you want to configure.

Step 2 Click **Security>Configure**.

The **Configuration Versions** window opens.

Step 3 Double-click **Intrusion Detection** under the currently applied version.

The **Intrusion Detection** dialog box opens.

Step 4 Click the **Profile** tab.

Step 5 Fill in the following:

- Select **Profile based Configuration**.
- Under **Signatures to Disable**, disable individual signatures by selecting their check boxes.
- Under **Response**, click either the **Relaxed**, **Moderate**, or **Strong** option.

Step 13 To modify the alarm severity level and the action the Sensor should take, click the signature and click **Modify**. The **Attack Signatures Edit** dialog box opens (Figure 6-13). Make your modifications using this dialog box.

Note Actions other then **None** are not supported for the IDSM.

Doc: 3701
Fls: 1352
CPMI - CORREIOS
ROS Nº 03/2005 - CN

ECT 5164 Paulo CPL - AC

Figure 6-10 Intrusion Detection Dialog Box Profile Tab

Step 5 Select **Manual Configuration.**

The **View Sensor** button becomes the **Modify Signatures** button.

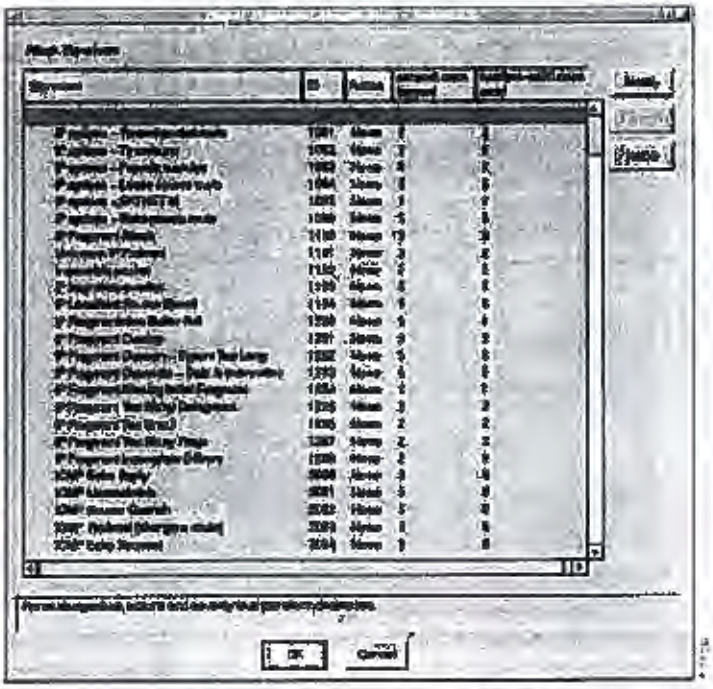
a. To modify Sensor signatures, follow Steps 6 through 10.

b. To modify IDSM signatures, follow Steps 11 through 18.

Step 6 Click **Modify Signatures.**

The **General Signatures** dialog box opens (see Figure 6-11).

Figure 6-11 General Signatures Dialog Box (Sensor)



Step 7 You can configure the action a Sensor takes when a signature detects misuse by clicking any **Action** field and choosing one of the following options from the drop-down list:

- **None**—Take no action.
- **Shun**—Shun the host.
- **Log**—Log the event.
- **Shun & Log**—Shun the host and log the event.
- **TCP Reset**—Close the TCP connection, but leave other connections alone.
- **TCP Reset & Shun**—Reset the TCP connection and shun the host.

Doc: 3701
Fls: 1353
CPMI - CORREIOS
ECT 15162 Paula SAC

- **TCP Reset & Log**—Reset the TCP connection and log the event.
- **TCP Reset, Shun & Log**—Reset the TCP connection, shun the host, and log the event.
- **Evidence Log**—This utility is deprecated and should not be used.

For each Sensor and Director in your organization, you can edit the **Severity Level**.

To find out more information about a signature, click its name in the listing and click **NSDB**. This will provide access to the NSDB through your HTML browser.

Step 8 Click **OK** to save your changes and close the **General Signatures** dialog box.

Step 9 Click **OK** to close the **Intrusion Detection** dialog box.

Step 10 To apply the configuration changes, click the newly created transient version on the **Configuration Versions** window and click **Apply**.

Note Clicking **Cancel** discards any configuration changes.

Step 11 Click **Modify Signatures**.

The **Signatures** dialog box opens.

Step 12 To modify attack signatures, click the **Attack Signatures** tab (see Figure 6-12).

Figure 6-12 Signatures Dialog Box Attack Signatures Tab

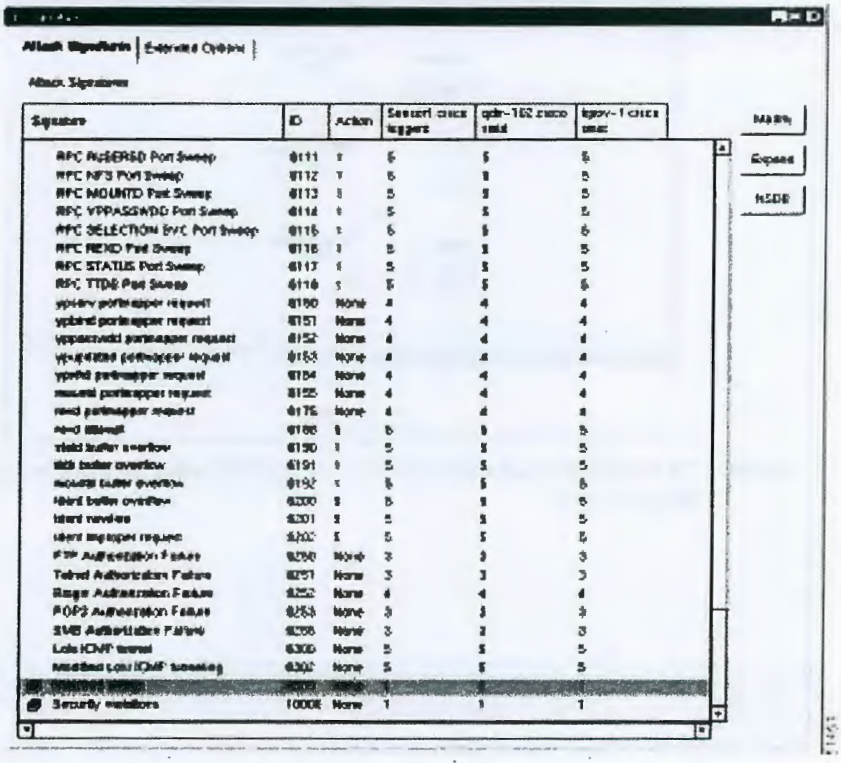
Step 13 To modify the alarm severity level and the action the Sensor should take, click the signature and click **Modify**. The **Attack Signatures Edit** dialog box opens (Figure 6-13). Make your modifications using this dialog box.

Note Actions other then **None** are not supported for the IDSM.

Doc: 3701
Fls: 1354
CPMI - CORREIOS
ROS Nº 03/2005 - CN

ECT 5160 Paulo AL - AC

Figure 6-12 Signatures Dialog Box Attack Signatures Tab

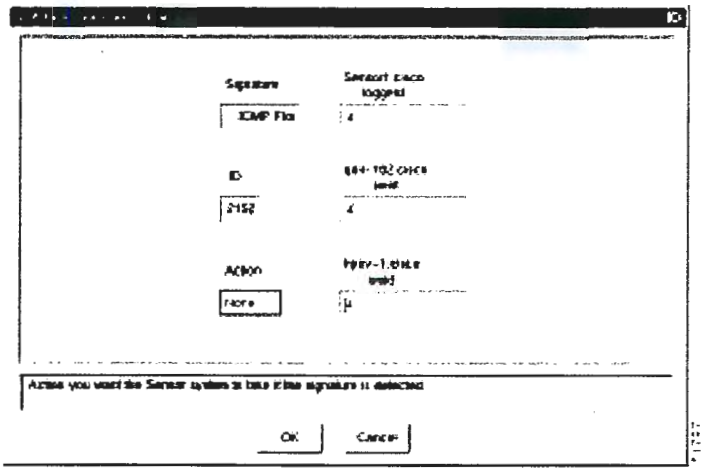


Step 13 To modify the alarm severity level and the action the Sensor should take, click the signature and click **Modify**. The **Attack Signatures Edit** dialog box opens (Figure 6-13). Make your modifications using this dialog box.

Note Actions other then **None** are not supported for the IDSM.

ECT I 5159 Paul CPL - AC

Figure 6-13 Attack Signatures Edit Dialog Box

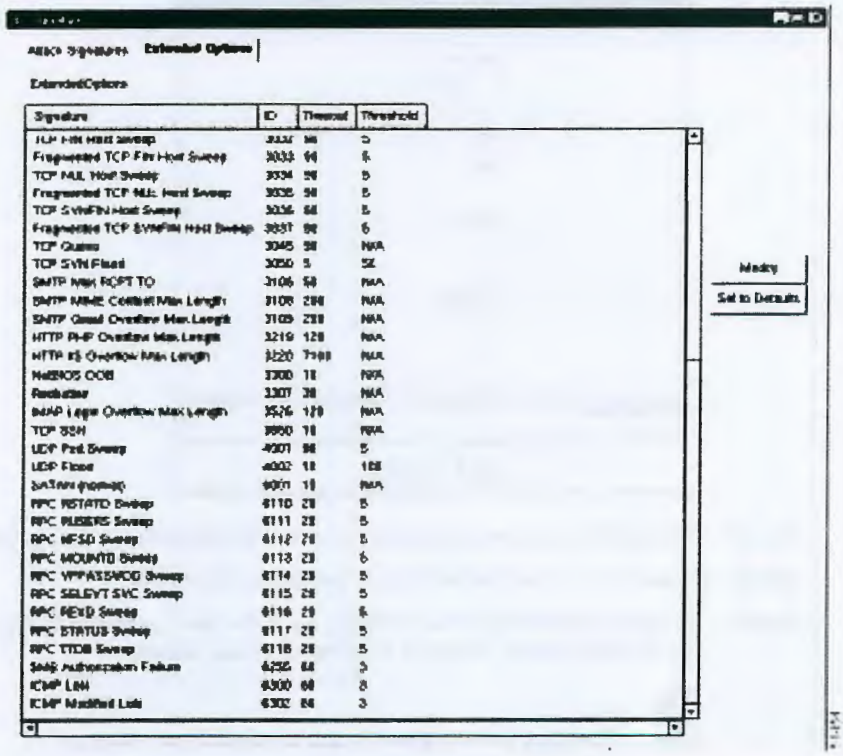


Step 14 To modify extended signatures, click the **Extended Signatures** tab (see Figure 6-14).

Doc:
Fls: 3701
1355
ROS Nº 03/2005 - CN
CPMI - CORREIOS

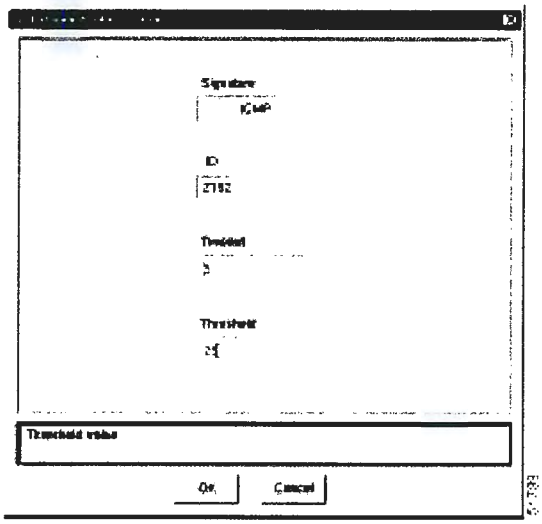
ECT
5158
Paula
CPL - AC

Figure 6-14 Signatures Dialog Box Extended Signatures Tab (IDSM))



Step 15 The **Timeout** and **Threshold** values can be edited by clicking a signature and clicking **Modify**. The **Extended Options Edit** dialog box opens (Figure 6-15).

Figure 6-15 Extended Options Edit Dialog Box



Step 16 Click **OK** to save your changes and close the **Signatures** dialog box.

Step 17 Click **OK** to close the **Intrusion Detection** dialog box.

Step 18 To apply the configuration changes, click the newly created transient version on the **Configuration Versions** window and click **Apply**.

Note Clicking **Cancel** discards any configuration changes.

Doc:
Fls: 1356 370
ROS Nº 03/2005 - CN
CPMI - CORREIOS

ECT
5156
Paula
CPL - AC

Advanced Intrusion Detection Settings

The **Intrusion Detection** dialog box also allows you to set up protected networks, name data sources for the Sensor, exclude patterns, and IP fragment reassembly.

Step 1 On the Director interface (NetRanger submap), click the Sensor icon you want to configure.

Step 2 Click **Security>Configure**.

The **Configuration Versions** window opens.

Step 3 Double-click **Intrusion Detection** under the currently applied version.

The **Intrusion Detection** dialog box opens.

Step 4 Click the **Protected Networks** tab.

Step 5 Click **Add** to enter the address and netmask of the network protected by the Sensor.

Step 6 To set up IP logging, click the **IP Logging Addresses** tab, then click **Add** to add addresses and networks you want the Director to IP log.

Note IP logging involves writing every incoming and outgoing packet to an IP session log with a naming convention of iplog.*Source_IP_Address*, where *Source_IP_Address* is the IP address of the source of the packets.

Step 7 Click the **Data Sources** tab.

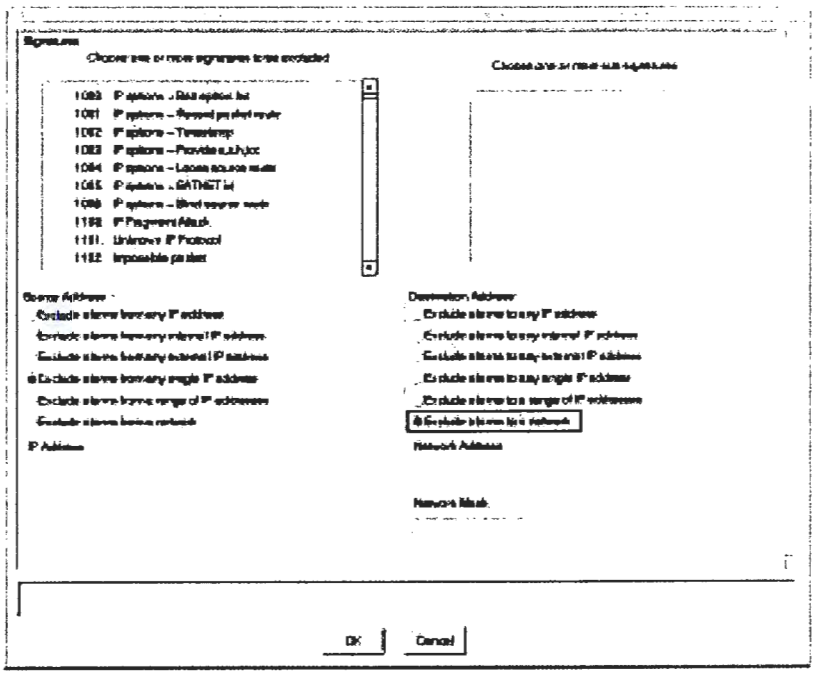
- If the Sensor is in standalone mode (for example, not working with a network device), then type the name of the Sensor's interface card performing packet analysis in the **Name Of Packet Device** field.
- If the Sensor is working with a router or packet filter, click **Add** under **Data Sources** and type the address and netmask of the managed network device.

Step 8 Click the **Excluded Patterns** tab.

Step 9 Click **Add** to set the signature ID, subsignature ID, source IP address or network, and destination IP address or network of any patterns you want to exclude.

The **Add New Enhanced Excludes** dialog box opens (see Figure 6-16).

Figure 6-16 Add New Enhanced Excludes Dialog Box



Step 10 Use the following values for the source/destination fields:

Note Only one of the following exclusions or tasks can be done at a time.

- Exclude alarms from any IP address (Source field = *)
- Exclude alarms from any internal IP address (Source field = *IN*)
- Exclude alarms from any external IP Address (Source field = *OUT*)
- Exclude alarms from a single IP address (Source field = *a.b.c.d*)
- Exclude alarms from a range of IP addresses; enter a starting and ending IP address (Source field =*a1.b1.c1.d1 - a2.b2.c2.d2*)
- Exclude alarms from a network address; enter a network address and a subnet mask (Source field = a.b.c.d/n, where *a.b.c.d* is the IP address and *n* is the number of 1s in the most signification portion of the subnet mask)

Doc: 3701
Fls: 1357
CPMI - CORREIOS
RGS Nº 03/2005 - CN

ECT 5154 Paula AC

Step 11 Click the **IP Reassembly** tab.

Step 12 Select the **Reassemble Fragments** check box.

Step 13 Set the following values for reassembly:

- **Maximum Partial Datagrams**—Maximum number of tokens that are in the process of reassembly at one time (default is 200 for the Sensor and 500 for the IDSM)
- **Maximum Fragments Per Datagram**—Maximum number of fragments that a datagram can have for the purpose of reassembly (default is 2000 for the Sensor and 190 for the IDSM)
- **Fragmented Datagram Timeout**—Ttimeout for the partial fragmented datagrams (default is 3 for the Sensor and 10 for the IDSM)

Step 14 For the IDSM, you can set up TCP Reassembly as follows:

- **TCP Three Way Handshake**—Watch for 3-way handshake related traffic (default is disabled)
- **TCP Strict Reassembly**—Watch the traffic when the receiver has sent an ACK for the TCP connection (default is **No Reassembly**)
  - **No Reassembly**
  - **Loose Reassembly**
  - **Strict Reassembly**
- **TCP Embryonic Timeout**—Timeout for partially open connections (default is 15)
- **TCP Open Establish Timeout**—Timeout for the established connections (default is 90)

Step 15 Click the **Port Mapping** tab (IDSM only)

Step 16 Set the following:

- **TCP HIJACK Ports**—Enter comma-delimited port numbers for ports that you want to be configured for TCP HIJACK
- **TCP SYNFLOOD Ports**—Enter comma-delimited port numbers for ports that you want to be configured for TCP SYNFLOOD

- **TCP Telnet Ports**—Enter comma-delimited port numbers for ports that you want to be configured for TCP Telnet
- **TCP HTTP Ports**—Enter comma-delimited port numbers for ports that you want to be configured for TCP HTTP

Step 17 Click **OK** to close the **Intrusion Detection** dialog box.

Step 18 To apply the configuration changes, click the newly created transient version on the **Configuration Versions** window and click **Apply**.

Note Clicking **Cancel** discards any configuration changes.

Configuring the System Files

The system files contain the information needed for IDS communication. You can access individual components by right-clicking them on the **Configuration Versions** window and clicking **File>Open**.

- **Authorizations**—The **Authorizations** dialog box contains a list of hosts that are able to configure the current machine, and what types of commands they are allowed to run:
  - **Get**—The **get** operation "gets" data related to certain functions, such as a single IP address from a shun list.
  - **GetBulk**—The **getbulk** operation operates like the get operation, but returns a list, such as an entire shun list of IP addresses.
  - **Set**—The **set** operation "sets" a value for a service or function, such as a netmask or IP address.
  - **Unset**—The **unset** operation "unsets" a previously set value.
  - **Exec**—The **exec** operation "executes" an action, such as enabling or disabling shunning.
- **Destinations**—The **Destinations** dialog box contains a listing of editable destinations for events (errors, commands, alarms, IP logs) on each host in the IDS.

Doc: 3701
Fls: 1358
CPMI - CORREIOS
ECT - CPL - AC 5152 Paula

- **Hosts**—The **Hosts** dialog box contains a listing of editable host names, organization IDs, and host IDs in the IDS.
- **Organizations**—The **Organizations** dialog box contains a listing of editable organization names and IDs in the IDS.
- **Routes**—The **Routes** dialog box contains a listing of editable routes in the IDS. The items in the listing include the following:
  - Host name
  - Connection number
  - IP address of host
  - UDP port number used for communication
  - A reserved type column, which should always have **1** as an entry
  - Heartbeat

Note The heartbeat is a time interval that *postofficed* uses when transmitting route verification messages. If the heartbeat is set to 5, then *postofficed* waits 5 seconds before transmitting another heartbeat. Furthermore, *postofficed* waits a period of time equal to three times the heartbeat interval for a response. If a response does not return in time, then *postofficed* assumes the route is down and sends an error alarm to the Director. The default heartbeat interval is 5 seconds, but you can raise this value if your network is congested. This allows a larger window for route verification.

- **Services**—The **Services** dialog box contains a listing of editable service names and service IDs on the IDS.
- **Signature Descriptions**—The **Signature Descriptions** dialog box contains a listing of editable signature names and signature IDs on the IDS.

Setting Up String Matching

This section provides a procedure for setting up corresponding RecordOfStringName and SigOfStringMatch tokens to detect and send alarms on the string "secret" used during a Telnet session.

To set up string match tokens, follow these steps:

Step 1 On the Director interface (NetRanger submap), click a Sensor icon.

Step 2 Click **Security>Configure**.

The **Configuration Versions** window opens.

Step 3 Right-click **Intrusion Detection** and click **Open**.

The **Intrusion Detection** dialog box opens.

Step 4 Click the **Profile** tab.

Step 5 Click **Manual Configuration**, and then click **Modify Signatures**.

The General **Signatures** (Sensor) or **Signatures** (IDSM) dialog box opens.

For the IDSM, click the **Attack Signatures** tab.

Step 6 Scroll down to **Matched Strings** and click it.

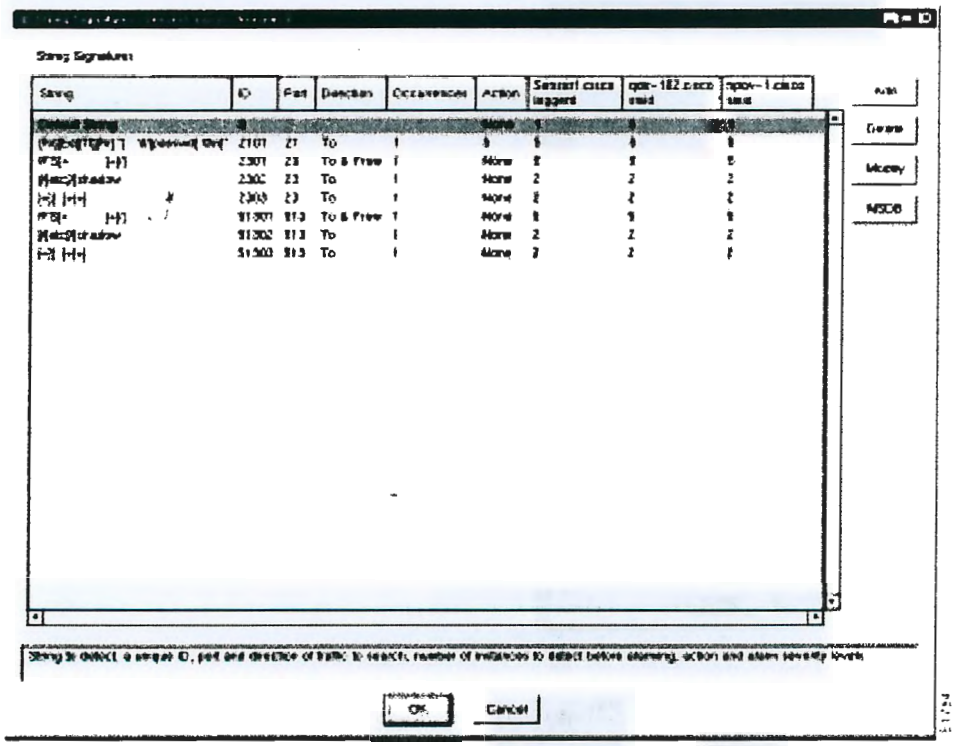
Step 7 Click **Expand** to open the **String Signatures** dialog box.

The **String Signatures** dialog box opens (Figure 6-17).

Doc: 3701
Fls: 1359
CPMI - CORREIOS
RGS Nº 03/2005 - CN

ECT 5150 Paula CPL - AC

Figure 6-17 String Signatures Dialog Box



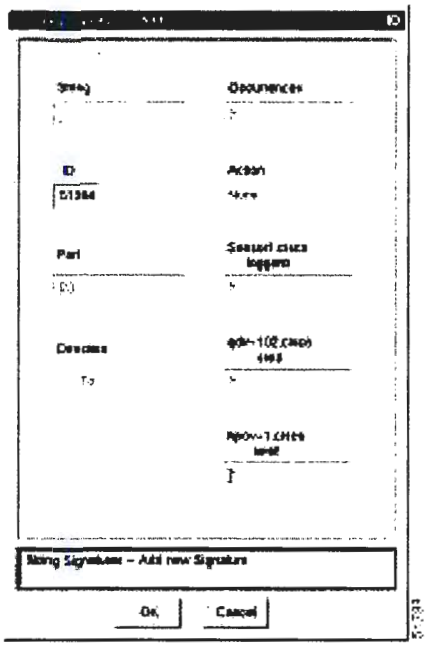
The **String Signatures** dialog box consists of a grid containing the following columns: string to search on, subsignature ID, port to scan, direction of traffic to scan, the number of string matches to allow before triggering an action, the action to trigger, and destinations for the data captured by the signature.

Step 8 Click **Add**.

The **Strings Signature Add** dialog box opens (see Figure 6-18).

FCT 5149 Paula CPL - AG

Figure 6-18 String Signatures Add Dialog Box



Step 9 Type `[Ss]ecret` in the **String** box.

This regular expression detects instances of the strings "Secret" and "secret."

A unique number is automatically generated in the **ID** box.

Step 10 Type `23` in the **Port** box.

TCP Port 23 is the well-known port for Telnet traffic.

Step 11 Click **To & From** in the **Direction** list.

Step 12 Type `1` in the **Occurrences** box.

Step 13 Click **Reset** in the **Action** list.

Step 14 Type `5` in each destination box.

Step 15 Click **OK** to save the new signature.

Step 16 Click **OK** to close the **String Signatures Add** dialog box.

Doc: 3701
Fls: 1360
CPMI - CORREIOS
ROS Nº 03/2005 - CN

E C T
5148
CPL - AC

Step 17 Click **OK** to close the **Intrusion Detection** dialog box.

Step 18 Click **Apply** on the **Configuration Versions** window to apply the new signature.

Each time the Sensor detects the string "secret" or "Secret" during a Telnet session, it now resets the user's TCP connection, and sends level 5 alarms to all destinations.

Running the HP OpenView Database Utility

You can run the HP OpenView Database Utility when you want to delete unwanted IDS alarms or repair database corruption. This section includes the following sections:

- Deleting Alarm Data
- Repairing Database Corruption
- Running the HP OpenView Cleanup Utility for Each Map

Deleting Alarm Data

If you want to delete IDS alarms only and the Director does not appear to be failing, follow these steps:

Step 1 Close down all instances of the HP OpenView user interface.

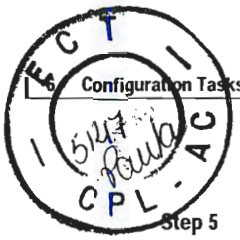
Step 2 Edit the $OV_REGISTRATION/C/nrdirmap file by removing the token `-Initial` from the line that begins with the word `Command`.

Step 3 Start the HP OpenView user interface.

Step 4 Click **Security>Advanced>OpenView Database (danger!)>Delete All Alarm Data**.

This launches the HP OpenView Database utility.

Note If you have multiple maps, use this option individually for each map.



Step 5 When the cleanup utility is finished, shut down the user interface.

Step 6 Put the `-Initial` token back in the nrdirmap registration file.

Step 7 Start up the HP OpenView user interface.

All IDS alarms are deleted from the HP OpenView database without deleting the hosts and applications that already exist.

Note The purpose of editing the nrdirmap registration file is to make sure that nrdirmap (the program that displays IDS data on the HP OpenView maps) is not running while the cleanup utility is running.

Repairing Database Corruption

When you have database corruption, you receive error messages in the errors.nrdirmap.* files similar to the following:

```
entityManager::createApplication, OVwDbGetFieldIntegerValue failed:
NULL field value
```

Note The message may vary slightly, but if the call begins with `OVwDb* failed`, you can assume there is database corruption.

To repair the database corruption, follow these steps:

Step 1 Close down all HP OpenView user interfaces.

Step 2 Run one HP OpenView user interface as user netrangr for a map that contains IDS data.

Note Make sure you have read/write access to the map (look in the lower corner of the map to make sure your access is not read-only).

Doc: 3791
Fls: 1361
ROS Nº 03/2005 - CN
CPMI - CORREIOS

ECT 5146 Paula CPL - AC

Step 3 Click **Security>Advanced>OpenView Database (danger!)>Delete All NetRanger Data**.

This launches the HP OpenView Database Cleanup utility.

The HP OpenView Database Cleanup utility deletes all the IDS data for this map from the HP OpenView database. A window opens telling you what is being deleted. The deletion does not cause problems with nrdirmap (the program that displays IDS data on the HP OpenView maps), because the error messages listed above confirm that nrdirmap has already stopped.

Running the HP OpenView Cleanup Utility for Each Map

If you have only one HP OpenView map with IDS data (you can see how many maps exist by typing `ovwls` from the command line), you do not need to do anything more. If you have more than one corrupted database, you must run the cleanup utility for each individual map.

To run the cleanup utility for each map, follow these steps:

Step 1 On the Director interface (NetRanger submap), to open each map with IDS data, click:

- **Map>Maps>Open/List** if your Director machine has HP OpenView 4.x or 5.x
- **File>Open** if your Director machine has HP OpenView 6x

The **Available Maps** dialog box opens.

Step 2 Click **Security>Advanced>OpenView Database (danger!)>Delete All NetRanger Data** for each of these maps.

The HP OpenView Database utility cleans each map that you select in the **Available Maps** dialog box. When the last map has been cleaned up, the utility reports that it does not need to run any more.

Step 3 Close the HP OpenView user interface.

Step 4 Restart the HP OpenView user interface.

Apêndice DB

RGS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1362
Doc: 3701

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.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1363
IPC-525
Fls:
3701
Doc:

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 DVMRP.

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]
```


ECTI 5144 Paula CPAL
RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1364
Doc: 3701

```
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.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
IPC-527
Fls: 3705
Doc:

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.

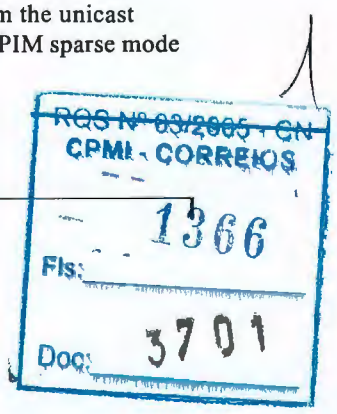
The basic DVMRP interoperability features are described in the section "Basic DVMRP Interoperability Configuration Task List" earlier in this chapter. To configure more advanced DVMRP interoperability features on a Cisco router, perform the optional tasks described in the following sections:

- 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:

ECT 5141 Paulo CPL AC
RQS Nº 03/2005 - CN CPMI - CORREIOS IPC-529 Fls: 1367 Doc: 3701

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 configuration 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:

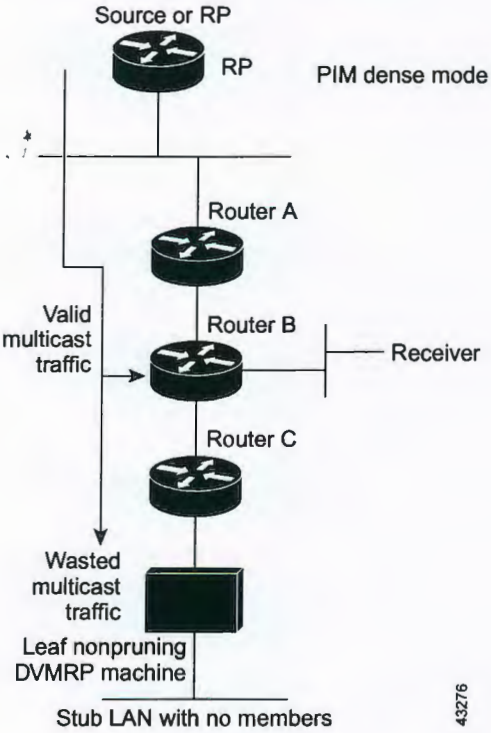
- When you specify the **in** keywordor no keyword, the *increment* value is added to incoming DVMRP reports and is reported in mrinfo replies. The default value for the **in** keyword is 1.
- When you specify the **out** keyword, the *increment* is added to outgoing DVMRP reports for routes from the DVMRP routing table. The default value for the **out** keyword is 0.

ECT 5139 Paula

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

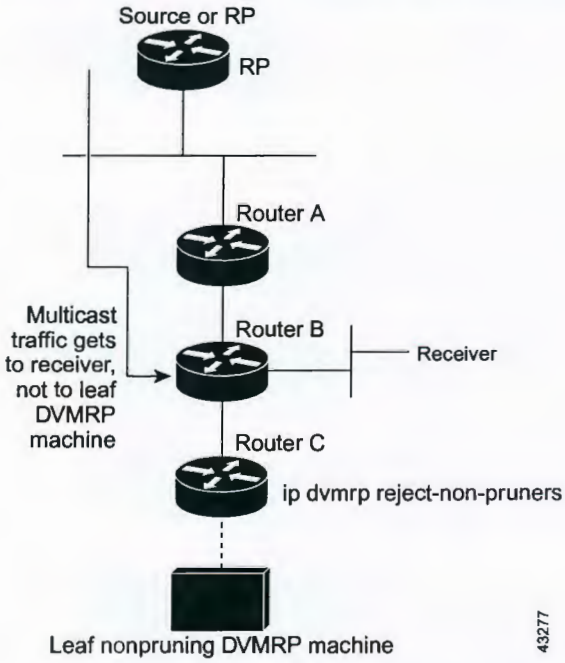


You can prevent a router from peering (communicating) with a DVMRP neighbor if that neighbor does not support DVMRP pruning or grafting. To do so, configure Router C (which is a neighbor to the leaf, nonpruning DVMRP machine) with the **ip dvmrp reject-non-pruners** interface configuration command on 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.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
IPC-531
Fls: 1369
Doc: 3701

ECT 5138 Paula CPL - AC

Figure 92 Router Rejects Nonpruning DVMRP Neighbor



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 that elapse between transmissions of sets of packets that constitute a report. The number of packets in the set 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.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1370
Doc: 3701

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
```


ECT 5137 Paula CPL - A
RQS Nº 03/2005 - CN
CPMI - CORREIOS
IPC-533
Fls: 1371
3701
Doc:

```
 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
```

Apêndice DC

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1373
Doc: 3701

ECT
5135
Paula
CPL - AC

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

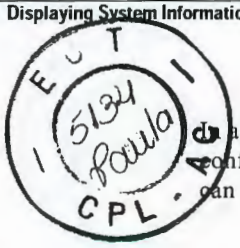
To manage network faults, you need to discover, isolate, and correct problems. You can discover problems with the system monitoring commands, isolate problems with the system test commands, and resolve problems with other commands, including **debug** commands.

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

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1374
Fls:
3701
Doc:

3701



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 command 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.

E C T
5133
Paula
D L . A C I

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

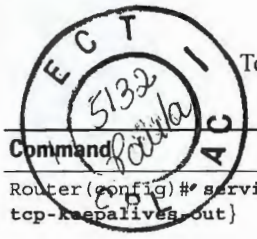
To test basic network connectivity, perform the tasks described in the following sections:

- 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.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1375
Doc: 3701



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
`ıter# 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.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
FC-289
Fls: 1376
Doc: 3701

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`	Enables log time stamps.
or `Router(config)# service timestamps log datetime [msec] [localtime] [show-timezone]`	

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:

RQS Nº 03/2005 - CN
CPMI - CORREIOS
FC-231
Fls: 3701
Doc:

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.

ECT 5127 Paulo L - A
RQS Nº 03/2005 - CN CPMI - CORREIOS FC-293 Fls: 1378 Doc: 3791

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 is 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.

E C T
1 5125
Paula
CPL - AC

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 | exit]`	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.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
FC-295
Fls: 1379
3701
Doc:

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.
`ıter(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
```


RQS Nº 03/2005 - CN
CPMI - CORREIOS
FC-297
Fls: 1380
Doc: 3701

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:

5121 Paula

```
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
```


RQS Nº 03/2005 - CN
CPMI - CORREIOS
FC-299
Fls: 1381
Doc: 3701

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:

RQS Nº 03/2005 - CN
CPMI - CORREIOS
FC-301
Fls: 1382
Doc: 3791

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.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
FC-303
Fls: 1383
Doc: 3701

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.

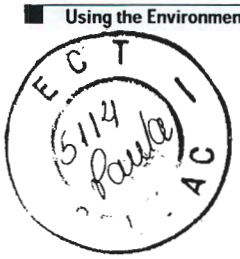
```
*Mar  1 00:05:51.443: %LINK-3-UPDOWN: Interface Serial1, changed state to down
*Mar  1 00:05:51.471: Se1 Debug: Condition 4, username fred cleared, count 1
*Mar  1 00:05:51.479: Vi1 Debug: Condition 2, interface Se1 cleared, count 3
*Mar  1 00:05:52.443: %LINEPROTO-5-UPDOWN: Line protocol on Interface 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.

Apêndice DD

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1385
Fls:
3701
Doc:

Apêndice DE

REQUERIMENTO Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1386
Doc: 3701

software loading capability for the hp tape array 5300

ECT
5113
Paula
CPL - AC

hp invent

hp surestore dvd-rom array module

The HP Surestore DVD-ROM Array Module further extends the versatility of HP's tape array solution. It provides DVD and CD reading functionality, and the ability to load software, all in a half-height form factor. This module is offline hot-swappable within an HP Surestore Tape Array 5300 for easy insertion and removal in a racked environment and offers the high performance (40x as a CD-ROM, 10x as a DVD-ROM) information services professionals need.

The HP Surestore Tape Array solutions provide a choice of rack enclosures in different heights to fit almost any data center. Available array modules encompass a wide range of tape drive technologies, as well as DVD-ROM, which can be mixed and matched in a single enclosure. The HP Surestore Tape Array 5300 offers upgrade options to enable SAF-TE remote manageability in a Windows® operating system environment and an additional power supply and fan kit for environments where redundancy is important.

key features/benefits

- **fast:** delivers high data transfer rates (10x for DVD-ROM, 40x for CD-ROM) for performance.
- **manageable:** offline hot-swap capability for easy insertion and removal.
- **flexible:** DVD and CD read functionality in a racked environment.
- **adaptable:** provides a half-height array module for addition to an HP Tape Array 5300.

specifications

Interface	Ultra SCSI LVDS. A fast, narrow, single-ended Ultra SCSI DVD-ROM with max throughput (burst rate) of 20 Mbps. Mounting in a Surestore DVD-ROM rack-ready module enables connection to an LVD SCSI bus for burst rates of 160 Mbps.	
Form Factor	5.25 inch, half-height	
Loading System	Slot disc loading system, long disc eject	
Insertion/Removal	Offline hot-swappable	
Performance	DVD-ROM: CAV 10x	CD-ROM: CAV 40x
Access Time/Seek Time	DVD: average 95 msec	CD: average 80 msec (random average)
Loading Time	Less than 3 sec (the period the disc starts to load and is clamped in the drive)	
Unloading Time	Less than 4 sec (from eject button press to disc unload)	
Disc Read Formats	DVD single layer & dual layer, DVD-R[1], DVD-RW[1], CD-ROM mode 1, XA mode 2, Photo CD (single & multiple session), CD-DA, CD-Extra, CD-R, CD-RW, Video CD	
Operating System Compatibility	Tape Array solutions are compatible with HP Servers running HP-UX, Windows®, Linux, and other industry-leading operating systems and software. For further information on system-specific compatibility visit: www.hp.com/go/connect	
Standard Warranty	3-years, next day[2] unit exchange, system matching on HP systems[3] (internal, external, and rack mountable units).	

[1] DVD-RAM is not supported.

[2] Unit exchange next day is not available in some countries.

[3] The system matching period applies to the host system standard warranty period only. The drive warranty reverts to unit exchange for the remainder of its standard warranty period after the host warranty expires.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1387
Fls: 3701
Doc:

specifications (continued)

Power		
Input voltage	+5VDC (+/- 5%), +12VDC (+/- 10%)	
Current draw:	+5VDC:	+12VDC:
Stand-by (average)	0.10A	0.05A
Read (average)	0.8A	1.3A
Maximum	1.2A	1.8A
Power Consumption		
Stand-by (average)	1.1W	
Read (average)	19.6W	
Maximum	27.6W	
Includes	Power save mode	
Physical Characteristics		
Weight	1.5 kg (3.3 lb)	
Dimensions (H × W × D)	42 × 165 × 320 mm (1.65 × 6.5 × 12.6 in)	
Safety		
Certifications	USA–UL (safety), Germany–TUV (safety), Canada–CSA (safety), EU–CE (safety & EMC), Australia/New Zealand–C-Tick (EMC only), Korea (EMC), Taiwan (EMC)	

ordering information

	Rack-ready DVD-ROM array module	C7499A
	Factory-racked DVD-ROM array module	C7499A-0D1
Accessories[1]	HP Surestore Tape Array 5300	C7508A

[1] Cables and terminators ordered separately.

HP Supportpacks

3-year, Next-day, Onsite Response	H3155A/E
3-year, Same day, Onsite Response	H4616A/E

more information

For more information on HP Tape Array products, contact any of our worldwide sales offices or visit the HP storage Web site at:
www.hp.com/go/storage

For information about hardware and software compatibility, visit the HP Storage Compatibility Web site at:
www.hp.com/go/connect

HP offers an extensive portfolio of HP and mixed environment storage specific consulting and support services to assist with your IT storage needs. For additional information, please contact your local HP representative or a worldwide sales office, or visit our Web site at:
www.hp.com/go/4service

hp invent

All brand and product names are trademarks or registered trademarks of their respective companies. Products may be shown with optional modules. The information contained in this document is subject to change without notice.

© Hewlett-Packard Co. 2001
Produced in USA 08-01
5980-6498EN

Single-System High Availability at the Forefront in Hewlett-Packard's Server Line

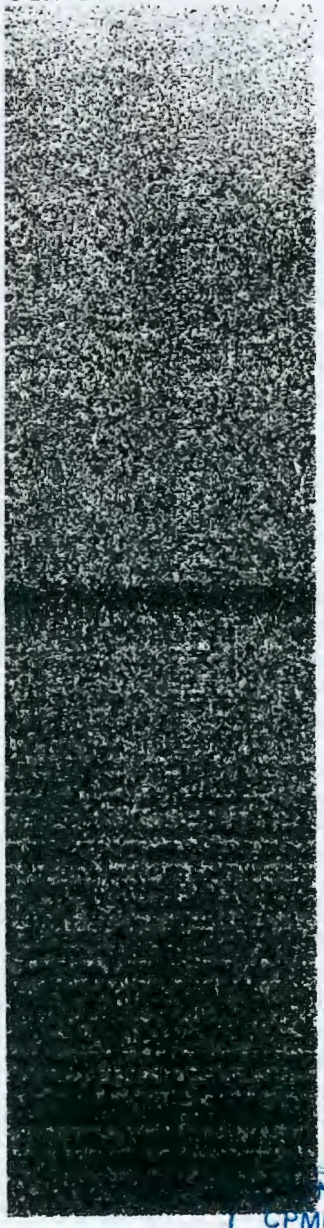
ECT
5111
Paula
CPL - AC

Prepared for Hewlett-Packard by:

D.H. Brown Associates, Inc.
222 Grace Church Street
Port Chester, NY 10573
(914) 937-4302
www.dhbrown.com

© 2001 D.H. Brown Associates, Inc.

October 2001



Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1388
Doc: 3701

TABLE OF CONTENTS

EXECUTIVE SUMMARY 1

INTRODUCTION AND OVERVIEW 2

Figure 1: HP's Tree-Based Server High Availability Architecture 3

HIGH AVAILABILITY: SERVER FAULT AVOIDANCE 4

HIGH AVAILABILITY: SERVER FAULT AVOIDANCE – RELIABILITY 5
Reliability – Hardware Quality 5
Reliability – Software Quality 6
Reliability – Patch Management 6
HIGH AVAILABILITY: SERVER FAULT AVOIDANCE – RESILIENCY 7
Resiliency – Dynamic Processor and Dynamic Memory Resilience 7
Resiliency – PCI Cards On-line Addition (OLA) 9
Resiliency – Fabric Resiliency 9
Resiliency – Auto-Deallocate 10
Resiliency – Hot Swap and Redundant Fans 10
Resiliency – Hot Swap and Redundant Power 11
Resiliency – Fault Tolerant SANs 11
HIGH AVAILABILITY: SERVER FAULT AVOIDANCE – ISOLATION 11
Isolation – Multipath I/O 12
Isolation – Auto Port Aggregation (APA) 13
Isolation – Dual AC Inputs 13

HIGH AVAILABILITY: SERVER SELF-HEALING 15

HIGH AVAILABILITY: SERVER SELF-HEALING – DISCOVER 15
Discover – Fault Management 15
Discover – High Availability Observatory (HAO) 16
Discover – Serviceability (System Configuration Repository [SCR]) 17
HIGH AVAILABILITY: SERVER SELF-HEALING – RESOLVE 17
Resolve – HPMC Analysis Tool 17
Resolve – Remote Administration/Remote Serviceability 18
Resolve – Online Journaled File System (JFS) 19
Resolve – Veritas Volume Manager (VxVM) 20
HIGH AVAILABILITY: SERVER SELF-HEALING – RECOVERY 21
Recovery – Boot Time Enhancement 21
Recovery – PCI Cards Online Recovery (OLR) 21
Recovery – Root-Disk Journaling 22

HIGH AVAILABILITY: SERVER DYNAMIC COMPUTING 23

HIGH AVAILABILITY: SERVER DYNAMIC COMPUTING – LOAD BALANCE 23
Load Balance – iCOD 23
Load Balance – Pay-Per-Use (PPU) 24
Load Balance – Process Resource Manager (PRM) 24
Load Balance – Workload Manager (WLM) 25
HIGH AVAILABILITY: SERVER DYNAMIC COMPUTING – DYNAMIC TUNING 26
Dynamic Tuning – Dynamic Tunables 26
Dynamic Tuning – Variable Page Sizing 26
HIGH AVAILABILITY: SERVER DYNAMIC COMPUTING – PARTITIONS 27
Partitions – Hard Partitions (nPARs) 27
Partitions – Virtual Partitions (vPARs) 29
Partitions – Processor Sets 31
Partitions – Partition Manager 32

ECT
1 5109
Paula
C.P.L. - AC

DISCUSSION AND CONCLUSIONS 34

APPENDIX: HP CROSSBAR-BASED BACKPLANE AND COMPETING BUS-BASED BACKPLANE 35

Figure 2: Simplified View of HP Crossbar-Based Backplane and Competing Bus-Based Backplane 36

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1389
Doc: 3701

Single-System High Availability at the Forefront in Hewlett-Packard's Server Line

EXECUTIVE SUMMARY

A vendor's ability to deliver high availability is key to the vendor's differentiation in the e-commerce world and other venues where downtime is dead time. Other variables such as technical excellence and cost-of-ownership are, of course, also important. However, given the business costs and other costs of a disruption, the pressure from corporate and information technology management, system administrators, and users the overwhelming factor is to have their systems highly available.

Hewlett-Packard has long recognized the need for highly available servers – even before the current industry emphasis on such capability. To provide its customers with the most available servers, HP has followed the guidelines of its internally developed high-availability infrastructure architecture. This infrastructure is modeled in the form of a tree with three main branches, each with three sub-branches. This is no mere theoretical construct; the sub-branches are populated with HP and third-party products that meet the practical, operational high-availability needs of HP customers.

For HP, server high availability is a multifaceted, holistic effort guided by a prime directive that the design-in of high availability into the server software and hardware architecture is fundamental. This principle results in literally hundreds of features and functions in each HP server that are dedicated to providing specific benefits to the server administrator and user.

As a result of HP's ability to implement and deliver on this philosophy, D. H. Brown Associates, Inc. (DHBA) believes that HP's high-availability architecture tree and its component parts provide an industry-leading model for the server community. The model is comprehensive and feature-function rich. This white paper provides an overview of this tree, its branches and sub-branches, and an overview of the component parts and their functionality.

After reading this material, the existing or potential HP server administrator or user, and numerous other interested parties in the IT community, will have a fundamental understanding of HP's high-availability efforts, why they are industry-leading, and what kind of benefits they offer.

Copyright 2001 © D.H. Brown Associates, Inc.

ECT 5107 Paula CPL - AC

INTRODUCTION AND OVERVIEW

A vendor's ability to deliver high availability is key to the vendor's differentiation in the e-commerce world and other venues where downtime is dead time. Other variables such as technical excellence and cost-of-ownership are, of course, also important. However, given the business and other costs of a disruption, the pressure from corporate and information technology management, system administrators, and users the overwhelming factor is to have their systems highly available.

Hewlett-Packard has long recognized the need for highly available servers – even before the current industry emphasis on such capability. To provide its customers with the most available servers, HP has followed the guidelines of its internally developed high-availability architecture infrastructure. This infrastructure is modeled in the form of a tree with three main branches, each with three sub-branches. This is no mere theoretical construct; the sub-branches are populated with HP and third-party products that meet the practical, operational high-availability needs of HP customers.

HP's "always on" vision includes Single-System High Availability (SSHA) and Cluster HA solutions. This white paper focuses on SSHA functionality and solutions.[1] There is, of course, much more to consider in order to provide high availability that is not discussed herein. For example, customers should keep in mind not only the overall HA solutions being offered by HP products (delivering both single-system and cluster HA), but also support services (such as Business Continuity Support or Critical System Support), IT processes support (consulting, disaster-recovery services, etc.), and partnerships with third parties (e.g., Oracle, Cisco, SAP) for fully integrated high-availability solution offerings.

For HP, server high availability is a multifaceted, holistic effort guided by a prime directive that the design-in of high availability into the server software and hardware architecture is fundamental. This principle results in literally hundreds of features and functions in each HP server that are dedicated to providing specific benefits to the server administrator and user.[2]

The conceptual and practical thinking behind the development of the tree components that provide these hundreds of features and functions is detailed in this white paper. After reading this material the existing or potential HP server administrator or user will have a fundamental understanding of HP's high-availability efforts, why they are industry leading, and what kind of benefits they offer.

---

1 MC/ServiceGuard is a specialized software facility that provides clustering and high-availability functionality for HP 9000 computer system products. MC/ServiceGuard is not discussed here.

2 These hundreds of features and functions are examined in detail elsewhere. Information about them is available from HP or DHBA.

Copyright 2001 © D.H. Brown Associates, Inc.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1390
3701
Doc:

ECT 5106 Paiub CPL - AC

HP breaks down its high-availability architecture concept into a tree structure with three main branches. These three main branches are each further broken down into three sub-branches (Figure 1: HP's Tree-Based Server High Availability Architecture). The main branches and sub-branches are:

- Server Fault Avoidance
  - Reliability,
  - Resiliency, and
  - Isolation.
- Server Self-Healing
  - Discover,
  - Resolve, and
  - Recover.
- Server Dynamic Computing
  - Load Balancing,
  - Dynamic Tuning, and
  - Partitioning.

The nine sub-branches are further broken down into multiple component parts per sub-branch as shown in Figure 1. This paper provides an overview of the 33 components made available in the nine sub-branches[3] and examines their administrator and user value.

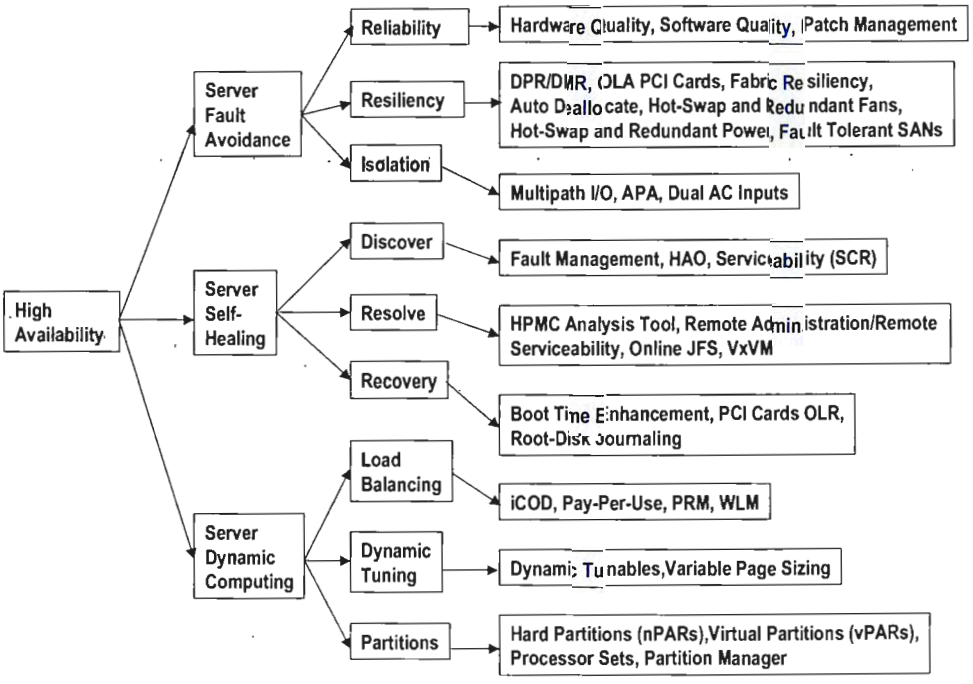


FIGURE 1: HP's Tree-Based Server High Availability Architecture

[3] The number of components will continue to grow.

Copyright 2001 © D.H. Brown Associates, Inc.

ECT 5105 Paula ACI

HIGH AVAILABILITY: SERVER FAULT AVOIDANCE

The sole purpose of HP's HA feature set is to address the real causes of customer downtime, as determined by actual field data. HP knows that delivering always-on solutions requires more than just delivering laundry lists of HA features with limited utility, or worse, HA features riddled with so many caveats as to render them useless. The real HA measure is how much uptime is seen by customer applications.

Avoiding faults is critical as the first line of defense to deal with server downtime causes. Crashing a system first, then dealing with recovery is not the optimum solution. Dealing with recovery, while important, should not be a primary HA strategy. Avoiding faults in the first place is key.

The term "failure avoidance" should not be confused with other schemes that provide standby hardware to be swapped in after a system crash has occurred. Sometimes, a server that is described as having 100% hardware redundancy in reality only allows for standby hardware to be swapped in – a less desirable condition. For HP, redundancy means that sufficient resources are available online to restore the system to proper operation without any application interruption.

HP's field data has shown that the primary causes of server hardware and/or software downtime is the following (roughly in order of occurrence):

1. main memory failures,
2. cache failures,
3. power supply failures,
4. I/O card errors,
5. sockets/interconnects,
6. networking/mass storage,
7. software panics,
8. ASIC/Backplane failures, and
9. clock failures.

The top seven items in the above list amount to 98% of downtime causes. Main memory and cache memory amount to about 50% of the fault-generation cases. Knowing this distribution, HP has addressed these failure sources to deliver the maximum availability with the features and functions described in the sections that follow.

Copyright 2001 © D.H. Brown Associates, Inc.

ROS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1391
Doc: 3701

ECT 5104 Paula CPL - AC

HIGH AVAILABILITY: SERVER FAULT AVOIDANCE – RELIABILITY

Reliability is the first sub-branch in the Server Fault Avoidance main branch of HP's availability tree. A reliability metric, and there are many, measures failures in a system, both hardware and software related. A highly reliable system has few failures of any hardware or software component (due to either planned or unplanned downtime).

HP pays major attention to its server reliability through robust system-architecture design, careful vendor and component selection, sophisticated manufacturing processes, and elaborate, time-tested software qualification and design processes. At the user production site, both hardware and software techniques work around failed components to reduce maintenance, the number of service calls, and warranty costs.

To better understand HP's reliability work, the next sections examine the issues of hardware and software quality. Then, patch management is detailed.

RELIABILITY – HARDWARE QUALITY

The first step in fault avoidance is using high-quality components in a server design. Toward this end, HP has implemented sophisticated field tracking processes that record and analyze all system and component failures in order to detect trends and provide feedback to allow the HP hardware design laboratory to build more robust future products. As a result of having this data, HP systems have been designed from the ground up to address these detected failure sources.

HP uses a number of hardware quality-ensuring measures designed to deliver reliable, high-quality servers. These measures include,

- a modular architecture to minimize server component count;
- a system design and qualification methodology that pushes the hardware to its maximum while running customer applications;
- provision for extensive component supplier qualification;
- use of high-volume blowers to maintain ASIC and CPU junction temperatures as cool as possible;
- vendor-selection processes that require demonstrated high-quality manufacturing processes, as well as demonstrated high reliability;
- vendor requirements to execute ASIC burn-in tests, which result in ten times the ASIC quality as compared to standard components;[4] and
- boards and systems receive HP burn-in, running customer applications, a process that weeds out early life failures.

[4] In contrast to non-burn-in.

Copyright 2001 © D.H. Brown Associates, Inc.

ECT 1 5103 Paula FL AC

RELIABILITY – SOFTWARE QUALITY

The best way to examine software quality is to directly query the software user. Who knows better than the user what is really going on as far as software quality is concerned? With the goal of going right to the user source for information, HP has conducted software quality studies at the Interex (HP Users Group) meetings.[5] As a result of HP's software quality emphasis, in the three years that the Interex study has been conducted, customer satisfaction with HP software quality and reliability has grown from 70% to 80%.

In a separate, randomized study this year (January 2001), overall satisfaction with HP-UX-based products is very strong with 71% of respondents indicating they are very satisfied, 23% indicating moderate satisfaction, and very few (less than 6%) indicating dissatisfaction.[6]

RELIABILITY – PATCH MANAGEMENT

HP employs a two-stage patch-testing process. When a defect or escalation is reported, it is important to respond quickly (especially if the defect is critical). This necessity for fast response must be balanced with the need for a high-quality patch whose delivery must not be delayed.

Understanding these criteria, HP has two patch models – reactive patch and proactive patch. The former is designed to solve an existing problem with timeliness as the highest priority – fix the problem the first time in a reliable manner and minimize change. There is some risk here since the fix speed may compromise complete patch testing.

A proactive patch is designed for preventive maintenance. With such a patch, reliability (rather than timeliness as is the case with the reactive patch) is most important. A proactive patch is a stable, tested patch. It is planned in advance, issued at defined times, and fully tested. The changes that occur because of the proactive patch are evaluated in advance and fully understood. Risk is minimized by full testing although large proactive patch use may still involve some risk.

A patch is put through a fix-creation process, a peer review, and the standard functional, and reliability testing for the subsystem that involves the patch. HP then releases the patch with a one star rating to indicate that it is for reactive patching only and to use it only if the problem is evident. One star patches are used only when two star or three star patches are not available.

---

[5] The study is conducted annually and the 2001 result included 2,533 participants who spend $9.3 billion on IT products ($3.3 billion on HP products).

[6] World-class performance on surveys such as this exceeds 50% in the very satisfied category, 90% in both the very and moderately satisfied category, and is 10% or less in the dissatisfied category. By far (48%), the primary reason that customers cite for being very satisfied with HP-UX products is high system availability. (HP support comes in second at 18%.)

Copyright 2001 © D.H. Brown Associates, Inc.

RQS Nº 03/2005 - CN CORREIOS 1392 Fls: Doc: 3701

ECT 5102 Faulk CPL-AC

A two star patch is a proactive patch that has met certain test criteria but is not fully qualified. It is to be used only when a three star patch is not available. The two star patch's probability of recall is typically 60% lower than that of a one star patch.

The patch then continues to be put through system testing in the HP enterprise patch test center, which duplicates the most common customer environments. Here it is bundled with other patches and the entire set is put through rigorous interoperability tests. This process typically takes five to eight weeks. At the successful conclusion of this testing the patch is rated three stars. Three star patches have 80% fewer recalls than do one star patches.

HIGH AVAILABILITY: SERVER FAULT AVOIDANCE – RESILIENCY

Even the highest quality components can, at some point, fail. Because of this fact, it is important to understand the failure rates of all components, understand the failure modes, and then design HA features to deal with these failure modes to minimize application downtime.

These points are captured in Resiliency, the second sub-branch of Server Fault Avoidance. Resiliency is the ability to keep running in the presence of faults so that applications see no downtime due to hardware or software failures. In a resilient server, work-arounds for problems are developed through a combination of redundant or self-correcting components and software techniques to enable transparent failover to a working component or system.

Good examples of resiliency technology are Dynamic Processor Resilience (DPR) and Dynamic Memory Resilience (DMR). The section that follows explains DPR and DMR. Subsequent sections provide explanations for the other five Figure 1 Resiliency components.

RESILIENCY – DYNAMIC PROCESSOR AND DYNAMIC MEMORY RESILIENCE

Dynamic Processor Resilience (DPR) permits a server to be resilient to the CPU cache errors that are a major contributor to system downtime. In an HP server with DPR, if a CPU generates cache errors at a predetermined, unacceptable rate, the CPU is automatically deconfigured, online. Moreover, to solve the problem, the server can be configured to automatically swap-in a spare CPU.

HP's server CPU caches are protected from single-bit hard errors and random soft errors generated from cosmic rays and other intermittent error-generation sources. Furthermore, the HP CPU has a physical cache layout that reduces the chance of a multi-bit error due to a random cosmic ray strike.[7]

[7] Cosmic ray strikes affect memory arrays by removing the charge on specific cell locations. In many cases, high-energy strikes can affect multiple physically adjacent bits. It is important to make sure (architecturally) that physically adjacent bits do not show up in the same logical cache line. Certain competing systems do not do this.

Copyright 2001 © D.H. Brown Associates, Inc.

ECT
I 5101
Paula
C L - AC

While CPU cache-error generation is an issue, main memory failure is the hardware event that causes the most customer downtime. HP addresses this failure mode with four features:

- memory chip spare,
- dynamic memory resilience (DMR),
- hardware memory scrubbing, and
- automatic deconfigure on reboot.

Memory chip spare is the server's ability to continue to run in the face of any single, or multi-bit chip DRAM error. HP server system DRAMS are set up as N+1 per set of 128 DRAMS per memory word since the firm believes this architecture is essential in the design of reliable memory systems. Systems without this functionality may fail at a high rate compared to HP systems with this functionality.[8]

Certain vendors deal with multi-bit SDRAM failures by accepting the fact that they will occur. This means that a scheme is used that supports failure detection, but not correction. This scheme, while it may be acceptable in low-end markets, is a dangerous choice for those customers who bet their business on not having any downtime. Systems based upon this corner cutting are at high risk to fail due to memory problems.

DMR represents the server's ability to online (i.e., while the application is running) deallocate failed memory pages. DMR is similar to DPR in that if a memory location is problematic (i.e., exhibits persistent errors), that memory will be online deallocated with no visible-to-the-user impact. HP believes that, as long as the server is shipped with adequate memory, it is likely that a failed memory will never have to be replaced over the product life. This likelihood results in a significant planned downtime reduction compared to non-DMR systems.

Aiding in this process is the hardware memory scrubber (available in the rp8400 and Superdome servers). The scrubber automatically corrects and clears single-bit errors in every memory line that is read by the CPUs. This is an advantage over most software-based scrubbers, which are limited to scrubbing only that memory which is not locked down by the operating system or an application.

Automatic deconfigure on reboot is the system's ability to dynamically remove failing memory during boot from the available memory pool without halting the entire system.

[8] HP has seen this at customer sites that use both the HP architecture and other architectures.

Copyright 2001 © D.H. Brown Associates, Inc.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1393
Doc: 3701

RESILIENCY – PCI CARDS ON-LINE ADDITION (OLA)

The PCI Cards OLA capability, the second Figure 1 Resiliency component, enables the online addition of PCI I/O cards to HP-UX-based servers designed to support this feature.[9] The server hardware uses a standard per-PCI slot power-control technology combined with operating-system support for the PCI Card OLA feature to allow the addition of a new card without affecting other components or requiring a reboot.

The OLA feature enhances server high availability by reducing both planned and unplanned downtime since the server can still run while an I/O adapter is added and configured. All HP PCI cards (including Gigabit Ethernet, Fibre Channel, SCSI, Term I/O) and their drivers support this feature.

As just noted, OLA can provide additional I/O resources and new I/O technology without a reboot. This means that administrators can add resources on demand, based on workload. As a result, the need for the difficult exact deployment planning of I/O cards in a server is reduced. Additional I/O cards can also increase the server availability by providing alternative failover paths.

RESILIENCY – FABRIC RESILIENCY

Fabric Resiliency is the third component of the Figure 1 Resiliency sub-branch. A fabric ties CPU and memory resources together. Moreover, if the server has partitions,[10] the partitions may share this fabric. If the fabric is not resilient, the server will suffer decreased uptime. Of course, from the server-functionality point-of-view, if the fabric is not resilient, neither are the server partitions. HP addresses fabric resiliency through four technologies:

- highly reliable fabric ASICs,
- redundant and hot-swappable DC-DC converters,
- hardware isolation between crossbar chips, and
- full end-to-end error correction.

HP's fabric backplane ASICs are manufactured and tested with processes that result in a ten-fold reliability increase over comparable ASICs not similarly manufactured with such expensive components and procedures. The result in the field is virtually zero backplane ASIC failure.

The DC-DC converters that power ASICs and other backplane chips are fully redundant and hot swappable.

This further adds to system availability, and significantly reduces shared failure modes between partitions. Only HP provides redundant power for backplane components; others provide redundancy only for clocks, which rarely fail.

---

[9] As of September 2001, this includes N-class, L-class, Superdome, and the newly released rp8400 servers.
[10] Different partition types are discussed later in this white paper.

Copyright 2001 © D.H. Brown Associates, Inc.

ECT 5099 Fls: ACI

The HP server backplane is built from crossbars with point-to-point connections. In a properly configured server, communication traffic in a partition is restricted to that partition so that there is no link sharing. Since each crossbar chip port is independent, the cells of different partitions coexist without affecting each other.

In competing bus-based servers, all domains participate in the communication coherency scheme and share address busses. This means that, in these systems, all domains are linked in some manner and there may be shared failure modes that can contribute to increased, unplanned downtime.

Figure 2 in the Appendix and its associated explanatory text provide a simplified example of both the HP crossbar-based backplane and a competing vendor's bus-based backplane, and how the HP approach provides superior high availability.

RESILIENCY – AUTO-DEALLOCATE

Nearly all HP server hardware is redundant.[11] The result is virtually zero failures that would keep a partitionable system down waiting for parts. If a component or entire subsystem fails self-test, for example, the server will automatically deallocate the faulty hardware, continue to boot, and run the application when the server partition (or server) comes up.

Auto-deallocate applies to CPUs, memory, fabric links, and I/O. Hardware redundancy accommodates PCI card I/O failures, the complete PCI chassis, or the connected cell board. With a properly configured I/O system, there is no failure that causes I/O loss.

RESILIENCY – HOT SWAP AND REDUNDANT FANS

All HP servers have redundant and hot swap fans. This design is fundamental to ensure the best server reliability. Certain HP servers, e.g., Superdome, have such high-capacity fans and blowers that sufficient airflow is provided for all conditions even in the presence of a failure. The new high-density HP rp8400 server is even more sophisticated. It takes a unique approach by adding special CPU fans to keep the CPUs cool even in the small rp8400 form-factor.

Heat is the mortal enemy of components that need to be as reliable as possible, so the heat issue in a high-density system requires special consideration. The rp8400's two-level cooling scheme offers the required cooling capacity at nominal cost. To accomplish this feat, the rp8400 uses turbo-cooler fans that draw air directly into the heat sinks of the critical CPU and cell VLSI chips.

At the extreme server operating-temperature ranges, the turbo-cooler fans maintain internal temperatures well below the design maximums. Under normal ambient operating conditions, turbo-coolers are not required. However, if the

[11] Minor exceptions include clocks and power-control circuitry that rarely fail (rated at a 1% per year failure rate).

Copyright 2001 © D.H. Brown Associates, Inc.

RQS Nº 03/2005 - CN CPMI - CORREIOS Fls: 1394 Doc: 3701

turbo-coolers run, the silicon operates well within its maximum lifetime thermal window. Again, the result is increased overall server-system reliability.

To further improve reliability, manageability software monitors the rp8400 fan speeds, including turbo-cooler fans. This software detects the first slowdown hint associated with fan bearing wear-out. As a result, the system administrator has an early alert (at least 100 hours) to the remote possibility of a turbo-cooler fan failure.

RESILIENCY – HOT SWAP AND REDUNDANT POWER

The front-end power supplies in all HP servers are fully redundant and hot swappable. The Superdome (high end) and rp8400 (midrange) servers also have redundant and hot swappable backplane DC-DC converters. The latter feature fully removes power conversion as a cause of multi-partition crashes. The rp8400 midrange server also has redundancy in many other areas of power conversion. This also contributes to its increased uptime.

RESILIENCY – FAULT TOLERANT SANS

Fault Tolerant SANs are the seventh, and last component of the Figure 1 Resiliency sub-branch. HP uses Fibre Channel technology for its SAN solutions and supports three Fibre Channel topologies – point-to-point, arbitrated loop, and switched-based fabric.

For the arbitrated-loop architecture, HP servers can interoperate with switches or hubs that have the Emulated Private Loop (or Quick Loop) feature. These switches regenerate the signals on each port (unlike passive hubs) and thus can stop bad signals or faults. For the switched fabric topology, links are point-to-point so that faults are inherently isolated.

HP-UX supports multipath I/O in both of the just-described fibre topologies. Such I/O can be used to ensure that there can be redundant links to a target and the target can be reached even if there is a fault in a SAN link or port. In all of these cases, administrators can use the fault tolerant and the multipath I/O technology to configure their SANs for maximum availability.

HIGH AVAILABILITY: SERVER FAULT AVOIDANCE – ISOLATION

Isolation is the third sub-branch of the Server Fault Avoidance branch of the HP high-availability tree. For HP, isolation means, for example, that each Superdome I/O slot has an independent I/O channel or PCI bus. This architectural design supports improved I/O performance since each PCI card can run at its full PCI speed and, at the same time, enjoy fault isolation.

Copyright 2001 © D.H. Brown Associates, Inc.

ECT 5097 Paula CPL - AC

When this capability is coupled with HP's Auto Port Aggregation (APA),[12] Logical Volume Manager (LVM),[13] and AutoPath, then Ethernet network links such as 100BT and Gigabit Ethernet, and mass storage links such as SCSI and FC can provide automatic failover, load balancing, and isolation from card or I/O bus failures. This capability contributes mightily to minimize application downtime.

ISOLATION – MULTIPATH I/O

A multipath I/O feature allows accessibility to a storage device or networking end-node through multiple paths. The access can be simultaneous (in an active-active configuration) or streamlined (in an active-passive configuration).

In a mass storage configuration, a disk LUN (Logical Unit Number) is reached from a controller via various switches or ports (i.e., for Fibre Channel) or via split cables (i.e., for SCSI). In a networking configuration (i.e., switched 100BT and Gigabit Ethernet), connectivity between two hosts may be achieved through various switches, routers, or controllers.

Care must be taken in these architectures to eliminate single-points-of-failure (SPOFs) between two end points. For further fault isolation, each PCI card resides on its own PCI bus. Therefore, all PCI card errors are contained on the card that generated the error and cannot propagate to other I/O cards.

The multipath I/O feature provides failover, load balancing, and failure isolation. Networking and mass-storage products such as APA and LVM provide path-failure detection and failover capabilities. Products such as APA/EMC-Powerpath/XP-Autopath can load balance among various paths. Failure to a path does not disrupt activities on other paths. This isolation is important for delivering high availability, since I/O is inherently error prone.

As an example of the above, consider a configuration wherein the APA product uses two Gigabit Ethernet adapters in an active-standby mode. The network is configured such that the two adapters can be connected to the same or different switches but can reach the same destination servers/clients. If one of the adapters/cables/switches fails due to an error, APA detects the error and can quickly route packets to the other adapter. Thus multiple paths greatly increase the system availability by providing redundancy and complete fault isolation.

[12] Discussed in the next section.

[13] Logical Volume Manager (LVM) is a subsystem for managing file systems and disk-storage spaces that are structured into logical volumes rather than being restricted to the beginning and end points of a physical disk. Logical volumes can be smaller than the disk or disk array on which they reside, or they can include all or part of several disks or disk arrays. Logical volume boundaries are not required to coincide with the boundaries of physical disks when multiple disks or arrays are used.

Copyright 2001 © D.H. Brown Associates, Inc.

RQS Nº 03/2005 - CN CPMI - CORREIOS
Fls: 1395
Doc: 3701

ISOLATION – AUTO PORT AGGREGATION (APA)

Auto Port Aggregation (APA) is an HP kernel-based networking product. It provides link aggregation, or trunking. This capability amounts to aggregation of two or more network physical ports into a single logical port (pipe). APA technology is transparent to higher-level communication protocol layers (e.g., TCP/IP).

APA is a cost effective software solution for upgrading to higher bandwidth while maintaining an existing infrastructure and providing a quick (less than a second), and easy failover mechanism. Links can be aggregated on an active-active basis or an active-standby basis.

Aggregation on an active-active basis helps in load balancing among links. APA can be configured to use several different load-balancing algorithms[14] for outbound traffic (depending on the configuration). Inbound traffic load balancing depends on the support of this feature by the infrastructure switches. Aggregation on an active-passive basis helps in the failover scenario. APA can automatically detect failures and failover to a standby link within one second (with minimal or no application disruption).

Administrators use APA to provide load balancing among similar links and also as a quick transparent failover mechanism. High bandwidths can be achieved by combining several low-bandwidth links together from the existing infrastructure.

ISOLATION – DUAL AC INPUTS

The HP 9000 Superdome server family was the first in the industry to achieve an Uptime Institute certification for fault-tolerant power compliance.[15] The second

[14] *Server-to-Switch: MAC-Based*
This algorithm balances the load by hashing the eight least significant bits of the destination MAC address stored within an Ethernet packet. It then directs the packet to a specific link within an aggregate. This algorithm is most optimal when used in environments that contain no routing between the server and the clients.

Sever-to-Router: IP-Based
This algorithm balances the load by hashing the eight least significant bits of the destination IP address stored within an Ethernet packet. It then directs the packet to a specific link within an aggregate. This algorithm is most optimal when used in environments that contain routers between the server and clients.

Server-to-Server: CPU-Based
Ethernet packets do not contain a CPU ID. For this reason, the CPU-based algorithm makes a separate system call to obtain the originating CPU ID for each thread. It then uses this CPU ID to direct the thread to an Ethernet port assigned to that CPU by the APA software.

Server-to-Server: TCP/UDP Port-Based
This algorithm uses the TCP/UDP source and destination port numbers to distribute traffic across the ports in a Link Aggregate. This algorithm is intended to be used in networking environments where direct Server-to-Server Link Aggregation is needed. However, this algorithm may also be used in place of the MAC, IP, or CPU-based algorithms.

[15] The Uptime Institute developed its fault-tolerant power compliance specification in cooperation with members of the Site Uptime Network and major hardware manufacturers. The Site Uptime Network includes 48 Fortune 500 companies. The specification is available at www.uptimeinstitute.com.

Copyright 2001 © D.H. Brown Associates, Inc.

ECT 5095 Paula CPL - AC

is HP's new rp8400. In fact, these HP server systems are the only currently available servers fully compliant with this standard for dual, fault-tolerant AC inputs. Compliance means that HP's servers can be powered from two fully independent input power sources that do not need to be in-phase.

The tests passed by Superdome and the rp8400 include a variety of power-source conditions that contain abnormal out-of-tolerance voltages, faulted AC power sources, brownout conditions, and more. As required, the Superdome family operates with no data loss and no performance degradation, as initially installed or at its ultimate capacity.

HP believes that as a result of the Uptime Institute's certification, HP's customers can minimize power-fault uncertainty as another step toward decreased unplanned downtime. Server systems lacking such certification may be susceptible to AC faults that allow data loss and hardware and/or performance degradation. In some cases, power-distribution difficulties may be generated for a site's facility-engineering team if the server power source is not as capable as the Uptime Institute requires it to be.

Copyright 2001 © D.H. Brown Associates, Inc.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1396
Doc: 3701

ECT CPL. AC

HIGH AVAILABILITY: SERVER SELF-HEALING

HIGH AVAILABILITY: SERVER SELF-HEALING – DISCOVER

As indicated in Figure 1, HP breaks down the Server Self-Healing branch of its high-availability tree into three sub-branches – Discover, Resolve, and Recovery. The Discover sub-branch has three components – Fault Management, High Availability Observatory (HAO), and Serviceability (System Configuration Repository, [SCR]).

The following sections discuss how HP-UX helps administrators discover server problems. They can set hardware monitors using HP Fault Management, which will then alert them to potential problems. They can also have HP proactively discover server problems via the High Availability Observatory (HAO) suite of support software and technologies. Administrators can also discover problems themselves by taking snapshots of their inventory using HP's System Configuration Repository (SCR) tool and analyzing the resultant data.

DISCOVER – FAULT MANAGEMENT

Fault Management is the name given to HP's overall strategy and program to provide a value chain for detecting, notifying, and repairing server problems so that uptime is maximized. Proper Fault Management requires working with hardware and operating-system designers from the beginning of a server design to create hardware and software capabilities and instrumentation points that create the ability to detect and isolate server anomalies.

For example, HP creates monitors to poll server health information or to asynchronously respond to server instrumentation points designed to report problems or faults. Fault Management also implements several methods for maintaining historical event information for trend analysis. Faults that generate errors and warnings are automatically logged to the syslog. Notes and audit information are logged to an event log.

Fault Management provides alerts to potential problems, as well as to occurring problems as soon as they are detected so that administrators can take corrective action. In some cases fault monitors are smart enough to repair or prevent future faults from occurring. Fault Management currently uses the HP Event Monitoring Service (EMS) infrastructure for its notification methodology. EMS enables a wide variety of notification methods (e-mail, SNMP traps, system console, system log, text logfile, TCP/UDP, and OpenView OPC messaging).

Fault Management events can be viewed and browsed directly by the administrator on a functioning server. Alternatively, the administrator can install HP's TopTools Management server and aggregate information from multiple systems in a domain. There is also the option to integrate Fault Management

Copyright 2001 © D.H. Brown Associates, Inc.

ECT 5093 Paula CPL - AC

events with enterprise-management software like HP's OpenView Operations or other enterprise-management software from BMC, Tivoli, Computer Associates, or MicroMuse.

When HP Support is purchased, Fault Management events can be forwarded to the HP Support Organization. HP can then monitor, filter, and "trend" the events and take action on items that need attention. At the premium end of HP's support offering for the ultimate in high availability, services may be acquired from HP's High Availability Observatory (HAO).

HAO provides continuous and proactive IT environment monitoring. HP uses a dedicated, private ISDN network that allows secure information flow between the customer site and HP's Support Organization and provides the HP Support Organization direct access to the customer's server. As part of the HAO implementation, HP installs a Support Node at the customer site, linked securely to HP.

Fault Management, together with its monitors, proactively reviews the health of server components and generates close to real-time events when problems develop. These events can trigger corrective action to enable the server to continue functioning, or they can trigger alerts to administrative personnel.

Fault Management furthers the philosophy of proactive as compared to reactive fault management. One of HP's high-availability goals is to continue to move in the direction of proactive fault management because of its ability to minimize downtime. HP's Fault Management system provides accurate problem diagnosis the first time, as the problem occurs. This results in a substantial decrease in any downtime associated with an event.[16]

DISCOVER – HIGH AVAILABILITY OBSERVATORY (HAO)

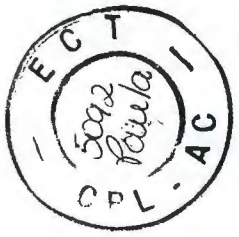
The High Availability Observatory (HAO) is a suite of support technologies, tools, and processes that HP provides to its customers with mission-critical applications. These customers include those with Business Continuity Support (UNIX only) or Critical System Support (UNIX or Windows servers). The combination of HAO technology, people, and processes in place provides a total HA solution. HP has quantified that HAO reduces resolution by approximately 40 minutes per case in which it is used.

The HAO consists of an HP-owned Support Node workstation and network router that resides on the customer site, a secure communication link back to HP's Mission Critical Support Center (MCSC), and equipment and software within the MCSC to maintain and analyze information about the customer servers. Configuration and status data from servers, software, and network interconnect devices is collected via the support node and securely transmitted to

[16] Data is available from HP to show this improvement.

Copyright 2001 © D.H. Brown Associates, Inc.

IRQS Nº 03/2005 - CN
CPMI - CORREIOS
1397
Fls:
Doc: 3701



the MCSC. This data is viewed by HP support engineers or securely shared with HP experts to help solve customer problems.

The data is also analyzed at the MCSC to alert HP and the customer of potential issues in their environment (e.g., bad patches or out-of-date firmware revisions). Hardware failure events within the customer mission- critical environment are detected by the HAO and alerts are sent back to HP for action.

DISCOVER – SERVICEABILITY (SYSTEM CONFIGURATION REPOSITORY [SCR])

HP's System Configuration Repository (SCR) is a no-cost tool that enables the collection of periodic or snapshot information about a server to a central database. SCR is a DMI management application. As such, SCR gets all the information it stores from standard APIs supported by HP's DMI service provider. The DMI service provider is SCR's collection agent on a managed node.

SCR accesses the DMI information available about a server and stores it as a snapshot in a central database. It follows the client-server model, i.e, a single server runs SCR and uses DMI to access client nodes. The information captured can be controlled, down to the level of each individual attribute, through the use of filters.

System administrators use SCR for troubleshooting. They can, for example, view their system state and compare it to previous known states (e.g., to determine that the correct state has been restored). System administrators also use SCR to generate system status, inventory, recordkeeping, and planning reports for internal (e.g., for change management) and external use (e.g., for third-party and purchase use).

HIGH AVAILABILITY: SERVER SELF-HEALING – RESOLVE

HP-UX provides capabilities and tools to resolve system problems. Toward this end, the Servicecontrol management-applications suite addresses the centralized configuration, fault, and workload-management requirements of an always-on Internet infrastructure and its servers. As indicated in Figure 1, the Resolve sub-branch of the Server Self-Healing branch has four components. The first of these components is the HPMC Analysis Tool part of the Servicecontrol management applications suite.

RESOLVE – HPMC ANALYSIS TOOL

The HPMC Analysis Tool automatically analyzes all server-stored error-log information after a catastrophic error. It is designed to describe the course of action to take to remedy the problem. This tool is useful for hardware problem diagnosis of those problems whose cause is not apparent through the system logs.

Copyright 2001 © D.H. Brown Associates, Inc.

E C T
5091
Paula
CPL - AC

The idea here is proactive rather than reactive diagnosis to avoid, where possible, of the need for service personnel to run time-consuming diagnostics. This tool is a safety net for those hardware problems that are not automatically detected and corrected by the server itself.

RESOLVE – REMOTE ADMINISTRATION/REMOTE SERVICEABILITY

The second component of the Resolve sub-branch is Remote Administration/ Remote Serviceability. Centralized web-based remote administration for HP-UX is delivered through the Servicecontrol suite of management applications. These applications include Ignite-UX, Software Distributor, System Configuration Repository, Servicecontrol Manager, Fault Management, Secure Web Console/Central Web Console, Partition Manager, System Administration Manager (SAM,) and MC/ServiceGuard.[17] These applications, either directly, or through Servicecontrol Manager integration, provide remote, web-accessible management.

- **Ignite-UX:** Ignite-UX allows remote image-based deployment. It also supports remote management of recovery images by collecting recovery images to a central server and then using them to repair systems remotely. Ignite-UX further provides the ability to ignite (cold install) client systems manually from the Ignite server console or automatically via the `bootsys` command.

  Such client-system installs are known as push installations. Ignite-UX can support multiple push installations in parallel. These parallel operations can, in turn, include multiple operating-system versions. Ignite-UX also provides the capability to ignite clients from a remote system, or ignite the client locally by "pulling" an operating system from an Ignite-UX server.

- **Software Distributor:** Software Distributor allows remote operating system and application installation and update. In addition to its ability to pull software from a central depot, Software Distributor also provides remote-operations features that allow software to be pushed to remote systems (targets) from the local host.

  These features and functions can be used interactively to monitor the results of all Software Distributor commands with the Software Distributor job browser GUI (graphical user interface) or the command line. Finally, Software Distributor can also deploy operating system and applications patches and, later, remotely roll back problematic patches (one at a time).

- **System Configuration Repository:** System Configuration Repository (discussed earlier in this white paper) collects and maintains hardware and software inventories from remote servers to a central repository.

- **Servicecontrol Manager:** Ignite-UX, Software Distributor, and System Configuration Repository applications independently support remote

[17] MC/ServiceGuard is well known and is not further discussed here.

Copyright 2001 © D.H. Brown Associates, Inc.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1398
Fls:
Doc: 3701

management. Through the Servicecontrol Manager umbrella, these applications are also available through a browser launched web interface. Other standalone HP-UX management applications are available remotely through Servicecontrol Manager integration. In fact, administrators can integrate and make available remotely (through Servicecontrol Manager's web interface) any standalone command line or X Windows-based application. With ServiceControl Managers' Distributed Tasks Facility (DTF), administrator scripts can be copied and executed across a set of systems easily and securely. ServiceControl Manager also supports a full command-line interface for further scripting of remote and multisystem management.

- **Fault Management:** Automatic rapid detection is a key contributor to high availability. Fault Management provides the framework and monitors to automatically generate events and forwards them to any enterprise-management system (e.g., HP's OpenView) or to a number of other notification methods.

- **Secure Web Console and Central Web Console:** Secure Web Console is a device that can either be embedded in certain HP Servers or attached to the console port for other HP servers. Secure Web Console provides secure web access to a console port through which the administrator gains access to an otherwise unavailable server. This access allows the reboot of a non-responsive system and interaction with the system-boot process. However, remote power-on is not supported.

  Central Web Console provides a console-consolidation capability for other console-access technologies such as terminal servers. With Central Web Console, large numbers of server consoles can be consolidated, managed and accessed from a common web-enabled interface. Central Web Console can use 3-DES encryption to encrypt the terminal-server session for secure access, including across firewalls.

- **Partition Manager:** For highly scalable servers, HP's Partition Manager is a web-enabled management interface for remote management of physical partitions. Once partitions are created all the Servicecontrol products and Servicecontrol Manager can manage each partition individually or together with Partition Manager (discussed later in this white paper).

- **System Administration Manager (SAM):** Running System Administration Manager (SAM) (through Servicecontrol Manager) provides system administrators with the ability to remotely manage server disks, file systems, peripheral devices, kernel configuration, users or groups, printers or plotters, and trusted-systems features. SAM is a GUI supplied with all HP-UX systems. SAM log files allow the tracking of system changes.

RESOLVE – ONLINE JOURNALED FILE SYSTEM (JFS)

Online Journaled File System (JFS), the third component of the Resolve sub-branch, provides the capability to perform system administration on a file system

Copyright 2001 © D.H. Brown Associates, Inc.

ECT 5089 Paulo CPL - AC

while it remains online and user-accessible. These system-administration functions include defragmentation, resizing, and online backup. Such capability allows optimum user-data availability while file-system downtime for maintenance is minimized.

With Online JFS, for example, disk defragmentation is eased. To resolve the fragmentation issue on a mounted file system, a defragmentation utility in Online JFS relocates data to remove unused space from directories, makes small files contiguous, and consolidates free blocks for file-system use.

Online JFS also provides backup capabilities. A snapshot or point-in-time image of a mounted file system may be made to provide a method for creating a backup (of selected files, a complete file system, or incremental backups).

Moreover, with Online JFS, file-system resizing is eased. Since file systems are originally created at a particular size, as system usage evolves the file systems may be too large or too small to accommodate changing usage patterns. Online JFS provides a method of solving these problems while the file systems remain mounted and user-available, e.g., the file system can be expanded or contracted. The fourth component of the Resolve sub-branch, the Veritas Volume Manager (VxVM), discussed in the next section, provides this specific capability.

RESOLVE – VERITAS VOLUME MANAGER (VxVM)

The Veritas Volume Manager allows (among other features) file-system resizing while the file system is mounted and user-available. The list below summarizes the VxVM capabilities.[18]

Veritas Volume Manager (VxVM) Functionality:

- dynamic reconfiguration of mirrors and volumes;
- support for multiple online data snapshots (for high availability and quick recoverability);
- automatic disk discovery (dynamic add of new disk arrays without reboot);
- hot sparing (allows administrator to designate disks in each disk group as spares);
- online relocation (add or replace or relocate disk drives while server is running); and
- disk group split and join (dynamic reorganization of disk groups).

[18] VxVM and the Veritas Cluster Volume Manager are integrated into MC/ServiceGuard.

Copyright 2001 © D.H. Brown Associates, Inc.

RQS Nº 03/2005 - CN CPMI - CORREIOS
Fls: 1399
Doc: 3701

HIGH AVAILABILITY: SERVER SELF-HEALING – RECOVERY

Recovery is the third sub-branch of the Server Self-Healing branch of the HP high-availability tree. To reduce unplanned down time, Recovery has three components provided by HP-UX 11i – Boot Time Enhancement, PCI Cards OLR, and Root Disk Journaling. These components decrease the time it takes to recover after a server or server-component crash.

RECOVERY – BOOT TIME ENHANCEMENT

Single-system boot time is the time interval from the initial power-on or reset of a system (i.e., a clean start state) to the time the system is available for the startup of services available on the network and/or user applications. Minimizing the time required for a server to boot up and become operational has a significant impact on the downtime associated with all single-server planned and unplanned downtime events. In other words, a boot-time reduction directly improves overall server availability while at the same time making planned events that require reboot more manageable.

Three software parts of HP-UX 11i are, or are being tuned to provide improved boot time. These parts are shown in the list below.

HP-UX 11i Boot Time Enhancements:

- ioscan-k option performance enhancement (both kernel optimization and ioscan command improvements);
- multiple SCSI LUN scanning (tuning SCSI LUNs scanning by leaving the target open for multiple LUN scans); and
- parallel I/O device scanning during boot (rather than serial scanning). The implementation is supported by enabling multiple threads early in the boot process.

RECOVERY – PCI CARDS ONLINE RECOVERY (OLR)

PCI Cards Online Recovery (OLR) enables the online replacement of PCI I/O cards on HP-UX-based systems designed to support this feature (i.e., as of September 2001, N-class, L-class, and Superdome). In operation, the server hardware uses the built-in per-PCI slot power-control hardware feature combined with operating-system support for the PCI Card OLR feature. This combination allows the replacement of an existing card without affecting other components or requiring a reboot.

This online-replacement feature allows increased availability since the server remains active while an I/O adapter is replaced. All PCI I/O cards (Gigabit Ethernet, Fibre Channel, SCSI, and 100BT) and their corresponding drivers support this feature. A replacement operation is limited to a like-for-like board replacement (i.e., the new card must be the same product as the replaced card).

Copyright 2001 © D.H. Brown Associates, Inc.

E C T
5087
AC

For those hardware environments where there are redundant link solutions, the I/O card replacement can take place without application impact.

RECOVERY – ROOT-DISK JOURNALING

Root-Disk Journaling, the third component of the Recovery sub-branch, enables fast file-system recovery after a system crash. Journaling, otherwise known as file-system logging, requires committing system writes to a sequential log file. Since the writes are stored on disk, not in system memory, the sequential nature in which they are written speeds up disk-write activity.

Note that VxFS (in JFS) uses a circular intent log. All file-system structure changes, or metadata changes, are written to this intent log in a synchronous manner. The file system periodically flushes these changes out to their corresponding disk blocks.

This journaling decreases the time it takes to recover after a crash (i.e., reduces unplanned downtime). Without such journaling, every block would have to be examined after a crash – a time-intensive process. With the use of an intent log, VxFS can recover from system downtime in a fraction of the time taken when an intent log is not used. The system simply scans the intent log, noting which file-system changes have completed and which had not. In some cases, the file system can roll forward changes to the metadata structures, because the changes were saved in the intent log. This capability adds availability and integrity to the overall file system.

Copyright 2001 © D.H. Brown Associates, Inc.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1400
Fls: 3701
Doc:

HIGH AVAILABILITY: SERVER DYNAMIC COMPUTING

HIGH AVAILABILITY: SERVER DYNAMIC COMPUTING – LOAD BALANCE

As indicated in Figure 1, the Server Dynamic Computing branch of the high-availability tree has three sub-branches – Load Balance, Dynamic Tuning, and Partitions. The sequel discusses how these three components increase a server's availability.

HP offers several schemes for system load balancing. For example, there is the flexibility to grow compute resources to meet business needs through purchasing more preconfigured (by HP) server capacity or by leasing compute resources. There are also techniques to optimize network bandwidth and load-balance network traffic across multiple similar links. Finally, administrators can focus the appropriate amount of compute resources on specific tasks and define service level agreements to ensure the system will automatically adjust these resources to meet the predefined needs.

HP's availability tree defines four components in the Load Balance sub-branch. These components are Instant Capacity on Demand (iCOD), Pay-Per-Use (PPU),[19] Process Resource Manager (PRM), and Workload Manager (WLM).

LOAD BALANCE – ICOD

Instant Capacity on Demand (iCOD) is an application program that allows the use of capacity already configured in a purchased system. Through iCOD, administrators purchase a specified number of activated processors, and pay a right-to-access fee for a specified number of deactivated processors. These deactivated processors can be activated at the user site, after which activation a fee is paid.

By preloading a system with additional capacity, the administrator enjoys the benefit of being able to add server-processing capacity (without reboot) and without having to pay until it is needed. In addition, there are high-availability benefits. An active processor identified as a potential failure can be automatically deactivated and replaced with an operational inactive processor. This capability allows a system to maintain full capacity and postpones the time when the system needs to be shutdown to replace the failing processor (perhaps until a regularly scheduled maintenance window).

On HP Superdome systems, the number of inactive processors is audited from a system perspective, not a partition perspective. This audit technique allows an administrator to perform load balancing between partitions by deactivating a

[19] Formerly known as Utility Pricing.

Copyright 2001 © D.H. Brown Associates, Inc.

E C T
5085
Paula
CPL - AC

previously active, but under-used processor in one partition, and activating a previously inactive processor in another partition. There is no cost to this procedure since the net total of server-active processors does not change.

iCOD is a quick, reliable way to add processing power. Physical addition of processor resources is (in relative terms) both time consuming and error prone, due to the procedure's manual nature. Whenever the server can be rebalanced without touching hardware there is an advantage.

LOAD BALANCE – PAY-PER-USE (PPU)

Pay-Per-Use (PPU) Pricing is an HP pricing model in which the administrator is charged for actual processor usage. The customer site acquires a specific hardware platform and number of processors, and is billed monthly for the actual usage, based on the number of active processors. The billing amounts vary, as processor usage increases or decreases. This billing model is, of course, different from the traditional financing approaches based on fixed payment amounts for the coverage period.

Where iCOD allows an administrator to respond to increasing processing demand by instantly activating and purchasing additional capacity, PPU allows flexibility in both usage directions – increased and decreased. When demand is high, additional processing resources are activated. When demand is low, excess processing resources are deactivated. For customers with a cyclic or unpredictable demand, PPU provides the flexibility to meet requirements without a permanent hardware investment to handle peak usage. PPU also has the high-availability benefit of replacing potentially failing processors with inactive processors (as does iCOD).

LOAD BALANCE – PROCESS RESOURCE MANAGER (PRM)

HP's Process Resource Manager (PRM) is a resource-management tool that allows a system administrator to focus the appropriate amount of server resources where the business at hand requires such resources. HP's PRM manages resources by partitioning a system based on PRM groups. A PRM group is a collection of processes that is assigned system resources. The system administrator assigns applications and users to PRM groups and establishes resource allocations for each group. PRM then manages each group's CPU, disk bandwidth, and memory resources according to the current configuration. The list below summarizes what may be done with PRM.

Process Resource Manager (PRM) Capabilities:

- *System Consolidation* – With HP's PRM, administrators can run multiple, mission-critical applications on a single system.
- *Response Time* – Administrators can improve the response time for critical users and applications through the use of PRM groups and assigned resources.

Copyright 2001 © D.H. Brown Associates, Inc.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1401
Fls:
3701
Doc:

- *Performance Expectations* – Administrators can set and manage user expectations for performance through the use of PRM groups and assigned resources.
- *Budget-Based Sharing* – With HP's PRM, administrators can allocate resources on shared servers based on how much of the server each department funded.
- *Convenient to Use* – Administrators can change the PRM configuration any time – even under load. Also, applications do not require modification to work with PRM.
- *Failover Recovery* – Administrators can ensure that an application package in a ServiceGuard cluster has sufficient resources after a failover.

LOAD BALANCE – WORKLOAD MANAGER (WLM)

HP-UX Workload Manager (WLM) supplements the functionality of HP's Process Resource Manager (PRM) by offering automatic resource-allocation and application-performance management through the use of prioritized service-level objectives (SLOs). The list below summarizes what may be done.

HP-UX Workload Manager (WLM) Capabilities:

- *Define SLOs* – With WLM, administrators can define and set priorities for goal-based and entitlement-based SLOs. Goal-based SLOs can be based on usage or performance. Entitlement-based SLOs allow administrators to specify a workload entitlement without specifying a goal.
- *Assign Multiple, Prioritized SLOs* – Administrators can assign one or more SLOs to a workload. The ability to assign multiple SLOs is helpful for workloads that require more than one SLO to accommodate a "must meet" goal and optional, lower-priority stretch goals.
- *Use GlancePlus Metrics* – For goal-based SLOs, administrators can use various GlancePlus metrics to define SLOs.
- *Assign CPU on a Per-Metric Basis* – WLM can grant a workload a certain amount of CPU as defined by a metric. For example, administrators can give a workload 2% of the CPU for each process in the workload group.
- *Manage Oracle® Instances* – Administrators can control Oracle instances and adjust their CPUs based on a number of factors. These factors include, among others, desired transaction response times, number of users connected, and whether a particular job is active.

Copyright 2001 © D.H. Brown Associates, Inc.

E C T
5083
Paula
C P L - AC

HIGH AVAILABILITY: SERVER DYNAMIC COMPUTING – DYNAMIC TUNING

Dynamic Tuning, the third sub-branch on the Server Dynamic Computing Branch of the HP availability architecture tree is an HP-UX capability that provides the ability to change the value of kernel tunables or memory page sizes without system rebuild or reboot. Dynamic Tuning has two components – Dynamic Tunables and Variable Page Setting.

DYNAMIC TUNING – DYNAMIC TUNABLES

Dynamic Tunables on HP-UX 11i provide the capability to change the value of certain kernel tunables without the need for system rebuild or reboot. Dynamic Tunables also provide the ability to ensure that changes to tunables are persistent across reboots.

Dynamic Tunables are supported via HP's System Administration Manager (SAM). As mentioned earlier, SAM is a GUI supplied with all HP-UX systems. Dynamic Tunables are also supported through a command-line interface. In addition, software developers can write software that changes tunable parameters.

Dynamic Tunables provide the ability to minimize downtime due to kernel reconfiguration. This capability increases the availability and productivity of HP 9000 users. Dynamic Tunables also allow easier kernel-configuration manageability by supporting commands and GUIs that align with work practices.

DYNAMIC TUNING – VARIABLE PAGE SIZING

Based on application-program heuristics and size, HP-UX dynamically, and by default, selects appropriately large page sizes for each memory object it accommodates. This use of larger pages conserves translation lookaside buffer (TLB) entries and reduces the occurrence of costly TLB misses. This capability improves the performance of many applications, particularly those with large reference sets and large amounts of contiguous memory (e.g., databases). Such increased performance provides increased availability since jobs complete more quickly.[20]

[20] HP 9000 systems with PA-RISC 2.0 processors support page sizes from 4 KB up to 1 GB in hardware. Starting with the HP-UX 11i release, HP-UX provided general support for variable-sized pages, thus allowing variable page size use on many user objects.

Copyright 2001 © D.H. Brown Associates, Inc.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1402
Fls:
Doc: 3701

HIGH AVAILABILITY: SERVER DYNAMIC COMPUTING – PARTITIONS

Partitions are the third sub-branch of the Dynamic Computing branch of the HP availability tree. There are four components to this sub-branch – Hard Partitions (nPARs), Virtual Partitions (vPARs), Processor Sets, and Partition Manager.[21] The HP family of partitioning solutions – HP's Partitioning Continuum for Always-On Infrastructure – provides, or will provide, Hard Partitions, Virtual Partitions, and Resource Partitions on an individual HP 9000 server node or within the HyperPlex (HP's 9000 Enterprise Server clustering implementation), as well as other HP server offerings including Superdome and the rp8400.

HP's various partitioning solutions offer the flexibility to execute multiple workloads on the same server while preserving application isolation. In fact, isolation between operating systems and applications is the great benefit of partitioning. Hard Partition (nPARs) hardware and software firewalls work together to provide the highest isolation possible within a server. HP software has been designed to operate completely within an nPAR and prevent any interference with other nPARs. In addition, hardware firewalls filter out all external traffic to ensure that wayward requests do not affect the partition.

In contrast to nPARs, Virtual Partitions (vPARs) allow multiple operating-system instantiations within an nPAR to provide software and application isolation. Each vPAR is isolated to the point that it can be rebooted, patched, and configured independent of all other partition vPARs.

For well-behaved applications, administrators use Processor Sets to assign compute resources to specific applications that run in the same operating-system environment. The Partition Manager configuration tool manages partitioned environments.

PARTITIONS – HARD PARTITIONS (nPARS)

An nPAR may be viewed as corresponding to a single, standalone system. Both Superdome and the rp8400 can be subdivided into partitions, each containing one or (usually) more cells that coherently communicate through the use of a high-bandwidth, low-latency crossbar fabric. Programmable hardware in the cells defines the partition boundaries so that the isolation is maintained from the actions of other partitions. Each partition runs its own independent operating system instance.

Hard partitions may be considered to be roughly equivalent to Sun domains. However the nPAR's architecture has several high-availability advantages. The use of nPARs in high-availability configurations requires the minimization or

[21] The partition concept is discussed in the HP white paper "HP-UX Virtual Partitions (vPARs)," September 2001.

Copyright 2001 © D.H. Brown Associates, Inc.

ECT 5081 Fls: AC

elimination of any possible shared failure modes between partitions. This minimization is not usually possible with Sun domains.

Typically, for example, other vendor-partition schemes use partitions that are involved in each other's coherency scheme. Therefore, any failure can theoretically cause the crash of multiple domains. Examples of this phenomenon include main memory multi-bit errors, cache errors, and backplane-addressing errors. This difficulty stands in contrast to HP systems for which extra care was taken to minimize the number of common components between nPARs, and to maximize the reliability of those that remain.

Also, unlike other systems with domains, the partitions in the rp8400 have hardware dedicated to guarding them from errant transactions generated on failing partitions. A failure in one domain will not affect any other domains. For example, each port on the crossbar chips is fully independent.

The hardware isolation provided by nPARs is ideal for datacenter simplification through server consolidation.[22] This is the case because each nPAR is free to run any operating-system type or version available, be it HP-UX, Windows, or Linux. Management and advanced-availability features are simpler and easier to implement on one larger system than on a group of smaller servers.

nPARs are also a win for product-development teams since they allow small development environments to sit alongside large production systems with complete isolation (thus conserving resources, ensuring high-availability levels, and more). The list below explains what accrues through nPAR use.

nPAR Capabilities and Benefits:

- Increase system usage through isolated hardware.
  - Partition a single physical server into several smaller servers.
  - nPARs have virtually no interaction and can be treated as independent servers.
  - Change capacity when needed by adding or deleting partition components.
- Increase flexibility through multiple, independent HP-UX, Windows, and Linux instances.
- Simplify the data-center.
  - Consolidate multiple servers into one server.
  - Add or change servers without changing the infrastructure or affecting other servers.
  - Capitalize on reliability and availability features offered by larger servers.

[22] DHBA conducts an on-going multi-client study of server consolidation and can provide information concerning this subject.

Copyright 2001 © D.H. Brown Associates, Inc.

RQS Nº 03/2005 - CN CPMI - CORREIOS
Fls: 1403
Doc: 3701

- Provide a server-independent easy upgrade path.
- Use GUI management tools to view the server group as one server.

PARTITIONS – VIRTUAL PARTITIONS (vPARS)

Virtual Partitions (vPARs) may be considered to be roughly equivalent to IBM LPARs. It is often necessary to dynamically create, modify, or delete the isolated operating environments on a running server without interrupting non-related partitions. Toward this end, HP developed HP-UX Virtual Partitions (vPARs). vPARs provide application (including name space) and operating-system isolation that runs on single-server nodes or nPARs (Hard Partitions on Superdome). Available for L3000, N-Class, Superdome, and future server nodes, vPARs are dynamically created using software commands. Each partition runs its own HP-UX 11i operating system (or later) image. Moreover, within each vPAR, up to 64 resource partitions can be created using solutions such as the earlier discussed HP-UX Process Resource Manager and Workload Manager.

vPARs allow an administrator to allocate a system-resource subset to each partition. In general, a vPAR owns a specified amount of memory, a specified CPU pool, and an I/O card set in the server.

In traditional server environments, all CPUs run the same operating-system instance and one or more applications so application or operating-system failures may affect the entire system. Running vPARs can limit the impact of such failures on application availability. For improved single-system availability vPARs allow an administrator to run one application per partition. Should a software failure occur in one partition, the application of that particular partition may be lost, but the rest of the applications on the other partitions continue to run. In fact, even if the operating system panics in one partition, applications running on other vPARs are not affected.

One of the inherent problems in a single system is the difficulty in expanding CPU resources when the demands of the application or multiple applications exceed the server's configuration. Usually the system needs to be shut down and additional CPUs added. With vPARs, a large server could have CPUs dynamically moved from one vPAR to another without bringing down the entire system. Resources can be moved to vPARs with the greatest demands, or removed when they are no longer required.

In a generic HP server without vPARs, the entire server is controlled by a single HP-UX instance. All of the resources (CPU, memory, and disk) are dedicated to the applications running in this single instance. The software stack for this server is traditional and consists of the application(s) talking to the operating system that communicates with the system firmware and hardware.

When vPARs are used the architecture is different. Consider, for example, a server divided into two partitions, each with a hardware subset (CPU, memory,

Copyright 2001 © D.H. Brown Associates, Inc.

ECT 5079 Paula L-AC

disk, etc.). Each vPAR will have its own boot disk, at least one CPU, one LAN connection and enough memory to run HP-UX and the applications intended to be hosted on the vPAR. As mentioned, each vPAR runs its own HP-UX copy (perhaps at different release or patch levels), and each is isolated from software errors, system panics, etc.

The software stack in the vPAR configuration has an application running in each of the two vPARs, each vPAR runs its own operating-system instance, and, importantly, each operating-system instance communicates with a single vPAR Monitor software layer which, in turn, communicates with the server's firmware and hardware.

This additional software layer, the Virtual Partition Monitor (vPAR Monitor), manages the partitioning of the resources, loads kernels, emulates global platform resources, and otherwise creates the illusion for each HP-UX instance that it is on a standalone system with only the resources that have been dedicated to that vPAR. Each HP-UX instance is unaware of the other system hardware while having complete ownership of the hardware resources it is assigned to. Note that the monitor is not involved in accessing I/O hardware or physical memory once it has transferred hardware ownership to a vPAR.

A partition database is at the heart of the monitor and it tracks what resources are associated with which vPAR. When the vPAR Monitor runs, the master database copy is kept in the monitor. All partition database changes are preserved across system reboots.

vPARs actually provide a tool that makes it possible to run multiple workloads. Each workload operates with its own unique operating-system configuration requirements on the same server at the same time. vPARs are also suited to make effective use of underused server nodes. Finally, they are ideal for testing new and/or enhanced products in a production environment. The list below shows what accrues through vPAR use.

vPAR Capabilities and Benefits:

- Increase system usage through partition of a single physical server or hard partition into multiple virtual machines or partitions (for L-Class, N-Class, and Superdome servers).
- Increase flexibility through multiple independent HP-UX instances and dynamic CPU migration across virtual partitions.
- Achieve greater isolation of applications running within separate operating-system instances within a single server, where each instance can be individually reconfigured and rebooted.
- Optimize application performance by adjusting operating-system resources. Tune the kernel differently in each Virtual Partition. This tuning eliminates the problems of trying to coax two different applications into running in the same operating-system environment when each application requires a different kernel parameter set.

Copyright 2001 © D.H. Brown Associates, Inc.

RQS Nº 03/2005 - CN CPMI CORREIOS
Fls: 1404
Doc: 3791

PARTITIONS – PROCESSOR SETS

HP-UX Processor Sets offer a mechanism to manage[23] system-processor resources among multiple workloads, users, and departments within an enterprise. A Processor Set represents an array of processors grouped together for exclusive access to applications assigned to that Processor Set. Processor Sets allow server partitioning into multiple Scheduling Allocation Domains such that workloads running in different Processor Sets do not contend with one another for server processor resources.[24] This capability also aids in server consolidation.

Processor Sets support dynamic-runtime reconfiguration. This means that a new Processor Set may be created, an existing Processor Set may be deleted, and a processor may be dynamically reassigned from one Processor Set to another (with access permissions). To accomplish this chore, the implementation of Processor Sets has a flexible ownership and access-permissions model. Every Processor Set has access-permission values that define who may change a configuration or who can execute the Processor Set workload. A Processor Set owner need not be a super user. This flexibility means that the need to completely rely on the administrator to control the Processor Set configuration and to assign Processor Set workloads is eliminated.

A server with Processor Sets capability is configured with one System Default Processor Set when it is started. All processors are assigned to this Default Processor Set. The Default Processor Set has its access permission set to allow all system users to execute their workload on the Default Processor Set processors. The Default Processor Set always has at least one processor, and is always available to all users and applications.

Processor Sets provide flexibility through set-able Processor Set attributes to allow administrators to control the server behavior. It is possible to anticipate and resolve this issue. For example, what happens if a person with permissions tries to delete a Processor Set that has a currently executing workload?

Processor Sets complement the fair-share scheduling CPU allocation mechanism available with PRM. In some instances it is better to allocate dedicated processors to workload via processor sets rather than using the default PRM scheduling. Processor Sets are integrated with the HP-UX Process Resource Manager. This means that a PRM group can be mapped to a Processor Set for processor resources rather than processor shares.

Processor Sets provide a flexible, lightweight mechanism to manage processor resources among multiple workloads, users, and departments. They allow consolidation of multiple independent applications on a single large server to avoid the need to maintain one server per application model. With their use, a

[23] HP-UX provides an API set to programmatically manage Processor Sets (along with system calls and a command-line program).
[24] Resource management based on Processor Sets is hardware platform-independent and can be used on any HP multi-processor system.

Copyright 2001 © D.H. Brown Associates, Inc.

ECT 5077 Paula CPL - AC

single large server can be shared among multiple departments rather than providing separate servers.

Organizations can have varying workloads depending on time of day, month, or year. As a result, the fact that Processor Sets allow dynamically changed resource allocations to workloads as needed without having to resource plan for the worst-case resource need of every workload is a major Processor Sets advantage.

Processor Sets can be applied to batch-processing workloads. In this scenario, a workload is assigned a Processor Set based on its resource needs. The configuration is changed to meet the needs of the next workload as the first completes. What is more, Processor Sets can provide processor-resource isolation for real-time applications to achieve better throughput response times.

PARTITIONS – PARTITION MANAGER

Partition Manager provides a GUI for managing Superdome servers that support nPARs. Partition Manager makes it easy to perform partition configuration tasks such as creating, modifying, and deleting partitions. Partition Manager also provides configuration and status information about a Superdome server. This information includes such high-availability information as the status of all power and cooling subsystems. In addition, Partition Manager includes automatic fault checking at its start up as well as on demand.

Partition Manager also performs a variety of high-availability-related checks whenever a partition is created or modified. These checks aid the administrator to ensure Superdome and partition availability.

The list below, Partition Manager Hardware Fault Checks, indicates the server hardware fault checks performed. The following list, Partition Manager Partition Fault Checks, indicates the performed partition fault checks. These two lists show that, in a variety of ways, Partition Manager alerts the administrator to situations in which the availability of the server, or a system partition, may be compromised.[25]

Partition Manager Hardware Fault Checks:

- Checks for power or cooling subsystems that contain failed or missing components (such as a failed fan or power supply). In addition to reporting failed or missing components, the checks also report if the subsystem redundancy is not at least N+1.[26] Thus, the administrator is alerted to potential availability problems before server operation is affected.
- Checks for cells with failed processors or memory DIMMs. Superdome systems are designed such that a partition boots using as many of the

[25] Note that all component failures also result in error notification via the chassis log mechanism, which can be monitored via the server's Service Processor user interface.

[26] N+1 indicates that a component can fail without affecting the subsystem operation.

Copyright 2001 © D.H. Brown Associates, Inc.

RQS Nº 03/2005 - CN CPMI - CORREIOS
Fls: 1405
Doc: 3701

resources assigned to it as possible. For example, if a processor has failed, the cell's remaining processors, memory, and I/O are still used. The Partition Manager fault checks help make sure that the administrator is aware that a partition is running with less than its resource complement.[27]

- Checks for failed crossbar ports. Such failures occur infrequently, and are reported via the chassis log mechanism. Here again Partition Manager provides redundancy for the administrator.

Partition Manager Partition Fault Checks:

- Checks for partitions with inactive cells, including an indication of inactivity as a result of incompatible cells within a partition. Proper partition configuration requires that all cells within a partition are compatible (e.g., same processor characteristics and system firmware revision). However, events can occur that break cell compatibility (e.g., upgrading system-firmware in only some cells). Thus, these checks alert the administrator to situations in which a partition is booted with less than its full resource complement.
- Checks for partitions with asymmetric memory configurations. Such a condition is not a failure, but could lead to less than optimal partition performance.
- Checks for cells with less than two working processors and cells with less than eight working memory DIMMs. A partition cannot use a cell if the cell has no working processors or no working memory DIMMs. Thus, the checks for at least two processors and at least eight DIMMs ensure that the cell could suffer a processor or DIMM failure (one DIMM failure results in a deconfiguration of the rank of four DIMMs containing the failed unit) and still be used by the partition. This procedure minimizes the potential loss of partition resources.
- Checks for partitions with less than two core cells. A partition must have at least one working cell that is attached to an I/O chassis with core I/O (such a cell is designated as the partition's core cell at boot time). Therefore, the check for a minimum of two possible core cells in a partition ensures that a partition can boot in the face of a cell, I/O chassis, or I/O card failure.

[27] Failures are also reported via the chassis log so that it is likely that the administrator knows that a failure has occurred. In this regard, the Partition Manager check is redundant.

Copyright 2001 © D.H. Brown Associates, Inc.

E C T
5075
Paula
L - AC

DISCUSSION AND CONCLUSIONS

High availability is the watchword for HP's server line. Cognizant of this watchword and recognizing that high availability is a key enabler that keeps its IT manager, system administrator, and end-user constituency content,[28] HP has maintained a company-wide effort to design in high availability from the beginning in its server software and hardware.

This design-in has been guided by HP's high-availability infrastructure model. This infrastructure, modeled as a tree architecture, has three main branches (Server Fault Avoidance, Server Self-Healing, and Server Dynamic Computing), each with three sub-branches and multiple components in each sub-branch (33 components in all). The overview of these components provided in this white paper indicates the breadth and depth of what HP makes available to its customers to ensure that highly available servers are a reality.

The effort to improve server availability is never-ending. Although, as this white paper demonstrates, HP is well situated with its current and forthcoming products, the firm cannot and clearly will not reduce its high-availability efforts as high availability continues to grow as an ever more important market differentiator.

HP has shown its ability to implement and deliver the real world, production-worthy components of its guiding high-availability architecture tree. As a result, DHBA believes that HP's efforts are a model for the server industry. The components are comprehensive and feature-rich. Although the hundreds of features and functions that these components deliver are not described here because of lack of space, the overview provided indicates the richness of the offering.

Now that this white paper is complete, DHBA believes that the careful reader (IT manager, system administrator, or end user) will have gained a fundamental understanding of HP's high-availability efforts, why they are industry leading, and what kind of benefits they supply.

[28] Nevertheless, this constituency always seeks ever-higher availability (at lower cost).

Copyright 2001 © D.H. Brown Associates, Inc.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1406
3701
Doc:

E C T
5073
Paula
AC

Full end-to-end error correction in the HP design means that all fabric data paths are resistant to both random single-bit errors and persistent single-wire "stuck at" faults. The fabric is therefore resilient to any single failure of pin, connector, socket, or soldering.

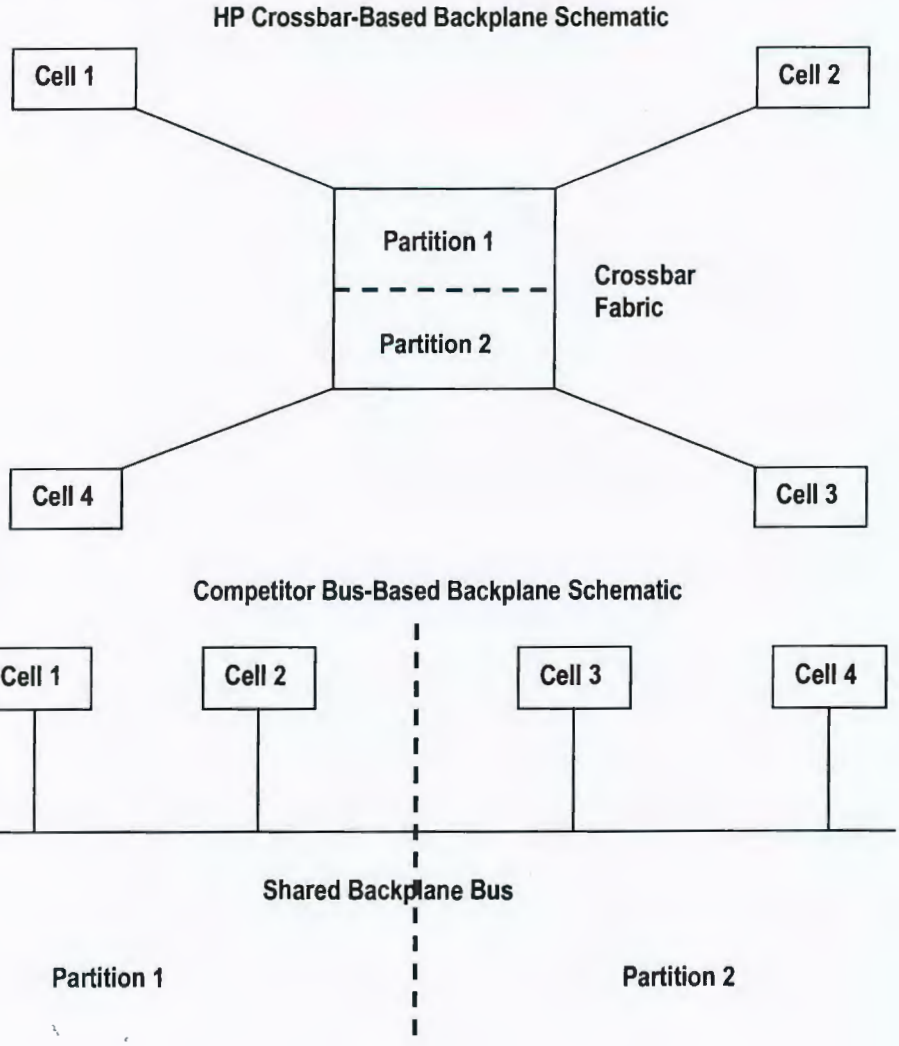


FIGURE 2: Simplified View of HP Crossbar-Based Backplane and Competing Bus-Based Backplane

Copyright 2001 © D.H. Brown Associates, Inc.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1407
Fls:
3701
Doc:

Apêndice DF

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1408
Doc: 3701

hp invent

hp StorageWorks disk system 2100

The feature-packed, worry-free HP StorageWorks Disk System 2100 delivers an industry-leading, high-capacity 1U storage solution. This entry-level, rack-optimized Disk System 2100 features open systems compatibility with HP-UX, MPE/iX, Windows NT®, Windows® 2000, Linux, NetWare, Solaris, and AIX, and offers the industry's lowest cost of entry. And because it's built with the HP commitment to developing dependable products and service, the HP StorageWorks Disk System 2100 ensures data integrity and manageability.

A fully loaded Disk System 2100 holds four 73.4 GB disks for a massive 293.6 GB of high-performance, upgradable storage. It also provides an impressive 160 MB/s transfer speed with built-in Ultra3 SCSI technology, all in a compact 1U package. For "set-it-and-forget-it" storage, your best choice is the HP StorageWorks Disk System 2100.

key features and benefits

- **large storage capacity**—293.6 GB of storage
- **space efficient**—1U of rack space
- **fast**—160 MB/s with built-in Ultra3
- **value for money**—daisy-chain multiple enclosures (up to 3 per HBA) for the cost of competing single-box systems
- **compatible**—works with any SCSI server or workstation
- **hot swap**—disk drives

technical specifications

disk drive capacity	**18.2 GB**	**18.2 GB**	**36.4 GB**	**36.4 GB**	**73.4 GB**
rotational velocity	10,000 rpm	15,000 rpm	10,000 rpm	15,000 rpm	10,000 rpm
transfer rate	160 MB/s	160 MB/s	160 MB/s	160 MB/s	160 MB/s
average seek time	5.2 ms	3.7 ms	5.2 ms	3.7 ms	4.9 ms

maximum enclosure capacity	293.6 GB
interface	Ultra3 SCSI
interconnect transfer speed	160 MB/s
connection	LVD–68 pin high density
daisy chaining	Yes–up to 3 per host bus adapter
certified operating systems	HP-UX, MPE/iX, Windows NT, Windows 2000, NetWare, Unixware, Linux, Solaris, SCO UNIX®, AIX

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1409
Doc: 3701

Apêndice DG

ROS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1410
Doc: 3701

APPENDIX: HP CROSSBAR-BASED BACKPLANE AND COMPETING BUS-BASED BACKPLANE

Figure 2 provides a simplified example of both the HP crossbar-based backplane (top) and another vendor's bus-based backplane (bottom). This Appendix describes how the HP architecture provides superior high availability.

Consider each system broken into two nPARs as shown in the figure. On the HP system, the crossbar logically separates the two physical partitions to provide performance and isolation. The competitor's shared backplane has all its cells competing for the same electrical bus. In this design, a snoopy bus-coherency scheme requires all transactions to be broadcast to and processed by all system cells. The high-queuing delays and saturation of the shared backplane bus can limit performance scaling.

To understand the reason for the just-made statements, consider a basic read from Cell 1 in Partition 1 of the crossbar-technology diagram to remote memory that resides on Cell 2 of Partition 1 of the crossbar-technology diagram. Partitions 1 and 2 are isolated by hardware firewalls. HP's crossbar switch and directory-coherency scheme allow the request to be sent only to the destination cell with data returning directly to the requesting cell. Remote memory traffic is restricted to the source and destination cells. The coherency directory is checked in the read-requesting cell and generates no additional traffic.

In contrast, for the same read operation, the competitor's shared backplane bus system must broadcast the memory read on the system address bus to all cells in the system to maintain coherency. Each cell must perform a snoop to determine whether or not the data is stored in its CPU cache and send coherency information to the read-requesting cell. Once the coherency data has been reported, the requested memory owner can return the data to the requester on the data bus. As noted above, scaling can be limited by queuing delays in the saturatable common bus. The snoopy coherency-scheme reliability and the need for bus-repeater chips limit availability.

A major weakness of the shared bus is that any failure during the read, either in the bus or during the coherency snoop, will result in crashing all cells in the system. At this point, the best that can be done is to deconfigure the broken hardware and reboot. Alas, downtime is a given in this design and has already occurred.

There is an additional partition-reliability benefit to the HP design. Unlike other snoopy coherency systems that must accept and respond to all coherency requests from all domains, HP server partitions have hardware firewalls. These firewalls are dedicated to guarding the server partitions from errant transactions generated on failing partitions. As a result, a failure in one server partition does not affect any other partitions.

Copyright 2001 © D.H. Brown Associates, Inc.

hp server connectivity

Ultra160 SCSI adapter

E C T I
5070 Paula
C P L - A C I
hp
invent

hp delivers performance and flexibility

two Ultra160 LVD SCSI channels on one PCI adapter doubles performance and saves valuable slot space

The HP A6829A PCI Dual-Channel Ultra160 SCSI host bus adapter delivers the performance and flexibility required for today's high-bandwidth servers. The 160 MB/second maximum data transfer rate across each of two independent Ultra160 SCSI buses makes it a perfect match for high-throughput applications such as data mining, streaming video, and scientific modeling. The A6829A adapter's 64-bit PCI interface maximizes the capability of the dual SCSI channels by increasing the throughput on the PCI bus to a maximum of 320 MB/second, preventing a system bottleneck from hindering data flow. This PCI interface doubles the PCI bandwidth from 133 MB/second to 266 MB/second, enabling maximum system throughput for both Ultra160 SCSI channels. This adapter also fits into 32-bit PCI slots, enabling users to qualify a single adapter for all server platforms regardless of the PCI architecture.

Complementing the Ultra160 SCSI offering is the HP A6828A Single-Channel PCI Ultra160 SCSI PCI host bus adapter—perfect for configurations requiring a single channel with all the features and functionality of Ultra160 SCSI.

With Ultra160 low voltage differential (LVD) SCSI technology, extended cable lengths of 12 meters for a fully loaded bus (or 25 meters for point-to-point connections) make this adapter ideal for disk clustering and RAID configurations.

The A6829A and A6828A PCI Ultra160 SCSI host bus adapters deliver superior I/O performance. Ultra160 technology doubles previous Ultra2 SCSI data transfer rates. With two channels, A6829A host adapter delivers up to 320 MB/second bandwidth.

The A6829A and A6828A PCI Ultra160 SCSI host bus adapters support both single-ended (SE) and LVD devices. When a single-ended device is attached, the card defaults to single-ended mode. With Ultra160 LVD devices, the adapter uses LVD mode and can perform at full Ultra160 speeds.

Ultra160 SCSI devices are widely available today. Ultra160 LVD is the industry standard for high performance and low cost. These adapters enable the best speed, compatibility, and technology available today. HP has led the way into Ultra160 LVD SCSI, while many of our competitors have been too slow to move to the latest technologies.

customer benefits

- up to 160 MB/s data transfer rate on two Ultra160 SCSI channels on a single PCI slot
- connect up to 30 SCSI devices (15 per channel)
- advanced multimode I/O supports Ultra160 LVD or legacy SE devices
- extended 12-meter cable length

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1411
Doc: 3791

application areas

Web-based Internet/intranet information distribution and transaction processing requires both fast response times and high availability. The Ultra160 SCSI host bus adapters make the SCSI link fast and reliable.

High productivity client/server systems require high-bandwidth, high-availability poths between the client, server, and data. The A6829A and A6828A with HP MC/Serviceguard and Logical Volume Manager (LVM) provide the high-speed, high-availability link between the server and the data.

Database backup demands very high bandwidth and availability to ensure one-pass backup. This is an ideal application for the HP Ultra160 SCSI adapters.

The A6829A and A6828A Ultra160 SCSI host bus adapters are perfect for solutions requiring high performance connections for voice, video, streaming, multimedia, and high-end applications.

All high-performance mass storage demands high availability and high throughput. The A6829A and A6828A Ultra160 SCSI host bus adapters meet the need.

features	benefits
Ultra160 SCSI host bus adapters	
two high-speed Ultra160 SCSI channels on one PCI card (A6829A)	• saves valuable PCI slots • wide Ultra160 LVD SCSI is the leading edge of SCSI performance and reliability
up to 160 MB/second maximum burst rate on each channel	• high-speed data transfer rates mean faster access to data and files • faster database queries and accesses • faster backup
mc/serviceguard and LVM	• high availability through automatic switchover to alternate adapter path
customer installable hardware and software	• easy customer installation and configuration means less reliance on HP assistance
multimode LVD (low voltage differential) and SE (single ended)	• backwards compatibility to SE enables easy integration with existing environment
long cable lengths	• up to 12 meters with LVD; increased cable length provides greater flexibility in system configuration, especially in clustering and RAID applications
up to 15 devices per channel in a daisy-chain fashion	• meets need for large disk arrays, multiple disks, and JBODs

specifications at a glance

host bus adapter card	A6829A	A6828A
PCI form factor	• standard PCI • L=8.95 in (22.7 cm) • W=4.25 in (10.7 cm) • H=0.72 in (1.8 cm)	• standard PCI • L=8.95 in (22.7 cm) • W=4.25 in (10.7 cm) • H=0.72 in (1.8 cm)
PCI	• PCI specification v2.1 • PCI 4X (64-bit, 66 MHz) • universal (3.3V and 5V)	• PCI specification v2.1 • PCI 4X (64-bit, 66 MHz) • universal (3.3V and 5V)
SCSI channels	• 2	• 1
connectors	• (2) external 68-pin VHDCI*	• (1) external 68-pin VHDCI*
configuration	• channels independently configurable	• channel independently configurable
termination	• active automatic termination • self-resetting term-power fuse	• active automatic termination • self-resetting term-power fuse

*VHDCI=very high density cable interconnect

platforms and maximum cards supported		
sx dome	• 96	• 96
rp8400	• 16	• 16
rp7400 series	• 12	• 12
rp5400 series	• 10	• 10
rp2400 series	• 3	• 3

operating system support		
hp-ux	• 11.0 and later	• 11.0 and later

environmental/regulatory specifications		
temperature	• non-operating: –40° to +70° C (–40° to 158° F) • operating: +5° to +40° C (41° to 104° F) • recommended operating: +10° to +40° C (50° to 104° F)	• non-operating: –40° to +70° C (–40° to 158° F) • operating: +5° to +40° C (41° to 104° F) • recommended operating: +10° to +40° C (50° to 104° F)
humidity	• recommended operating: 40% to 60% RH at 22° C (70° F)	• recommended operating: 40% to 60% RH at 22° C (70° F)
altitude	• 10,000 ft (3.1 km)	• 10,000 ft (3.1 km)
electromagnetic compotibility	• North America: FCC class A • international: EN 55022 class A	• North America: FCC class A • international: EN 55022 class A

cables/terminators		
recommended VHDCI to 68-pin HD SCSI cables		
C2361B	• 1.0m VHDCI to 68-pin HD	• 1.0m VHDCI to 68-pin HD
C2362B	• 2.5m VHDCI to 68-pin HD	• 2.5m VHDCI to 68-pin HD
C2365B	• 5.0m VHDCI to 68-pin HD	• 5.0m VHDCI to 68-pin HD
C2363B	• 10.0m VHDCI to 68-pin HD	• 10.0m VHDCI to 68-pin HD

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1412
Doc: 3731

specifications at a glance *(continued)*

cables/terminators *(continued)*		
recommended VHDCI to VHDCI SCSI cables		
C2372A	• 1.0m VHDCI to VHDCI	• 1.0m VHDCI to VHDCI
C2373A	• 2.0m VHDCI to VHDCI	• 2.0m VHDCI to VHDCI
C2374A	• 5.0m VHDCI to VHDCI	• 5.0m VHDCI to VHDCI
C2375A	• 10.0m VHDCI to VHDCI	• 10.0m VHDCI to VHDCI
recommended LVD/SE multimode SCSI terminators		
C2364A	• 68-pin HD LVD/SE multimode terminator	• 68-pin HD LVD/SE multimode terminator
C2370A	• VHDCI LVD/SE multimode terminator	• VHDCI LVD/SE multimode terminator

Note: This card is self-terminating when no cable is attached. However, a terminator is required on the final device in the SCSI chain. The appropriate terminator for that device should be ordered and utilized.

ordering information

A6829A or A6828A	
option #0D1	• factory integrated
option #AVN	• release notes

restrictions and limitations

• HVD (high voltage differential) devices are not supported

for more information

For additional information on this or other HP enterprise networking solutions, please visit us on the Web at **http://www.hp.com/go/hp9000io**, or contact any of our worldwide sales offices or HP Channel Partners.

(in the U.S., call 1 800 637 7740)

Technical information contained in this document is subject to change without notice. Performance information is estimated. Actual performance will depend on configuration.

© Copyright Hewlett-Packard Company 2002.

HP product information and technical documentation is available online. In addition, configuration tools and pricing information allow registered users to place orders online.

5981-0584EN

Apêndice DH

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1413
Doc: 3701

ECT I 5066 Paula CPL - AC

» return to original page

dual port 100Base-T and dual port wide ultra2 SCSI adapter

The demand for server resources is greater than ever in today's enterprise computing environment. Getting the most functionality, performance, and flexibility out of your computing resources is crucial to meeting this increased demand. The HP Dual-Port 100Base-T and Dual-Port Wide Ultra2 SCSI Adapter card gives you two high-speed network connections and two high-speed mass storage connections, all in a single PCI slot.

product information
» overview & features
» specifications
» information library

Servers supporting images, video, client/server applications, heavy LAN traffic, and databases require greater I/O bandwidth and connectivity. Data reliability, device connectivity, and cable lengths are often the issues with these critical systems. HP's Dual-Port 100Base-T and Dual-Port Wide Ultra2 SCSI Adapter provides impressive I/O bandwidth, high reliability, and 12-meter SCSI cable lengths in one standard PCI adapter. It is perfect for high-connectivity servers demanding high-speed LAN and SCSI connections.

The HP Dual-Port 100Base-T and Dual-Port Wide Ultra2 SCSI Adapter integrates nicely into existing infrastructures providing substantial cost savings. The auto-sense dual 100Base-T adapter can be immediately deployed in a 10Mbps environment. When the environment changes to 100Mbps, the adapter senses the new speed and you instantly have 10X the speed.

Ultra2 LVD SCSI is widespread in the marketplace due to its low power, high speed, and reliability. With the capability to multi-mode, this adapter is backwards compatible with SE (single-ended) SCSI devices.

The flexibility of this adapter is amazing. It can be utilized and integrated in a great variety of environments and solutions.

application areas

Web-based Internet/Intranet Information Distribution and Transaction Processing requires both fast response times and high availability. The HP A5838A LAN/SCSI Card with Auto-Port Aggregation software provides the increased bandwidth. With MC/ServiceGuard the A5838A provides high availability. The 10/100Base-T and LVD technologies improve overall speed and performance.

Client/Server systems require high-bandwidth, high-availability paths between the database servers and the application servers. The HP Auto-Port Aggregation and Ultra2 SCSI solutions are well suited for these popular high-productivity client/server application systems.

Database backup demands very high bandwidth and availability to ensure one-pass backup. This is an ideal application for the HP A5838A LAN/SCSI Card.

Multimedia transmission of voice, video and data requires high bandwidth and reliability. Again, HP A5838A LAN/SCSI Card meets these needs brilliantly, resulting in well-implemented multimedia applications.

features	benefits
A5838A Adapter Card	
Two high-speed Ultra2 SCSI ports and two 10/100Base-T RJ45 ports on one PCI card	• Saves valuable PCI slots by combining storage and LAN solutions onto one card. • Full-bandwidth power of two Wide Ultra2 SCSI and two 100Base-T LAN ports means faster Internet, Intranet, data, file, and application access, especially for multimedia and high-end apps. • Low-cost, high performance: 100Base-T technology is

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1414
Doc: 3701

	lower cost than FDDI or ATM. • Wide Ultra2 LVD SCSI is the leading edge of SCSI performance and reliability.
MC/ServiceGuard support	• High availability through automatic switch-over to alternate path in the event of a path failure.
HP's high power diagnostic, exerciser, and administrative software tools	• Easy customer installation and configuration. • Fast and easy LAN/SCSI management. • Tools compatible with those of LAN/9000.
Customer installable hardware and software	• Easy customer installation and configuration means less reliance on HP assistance.
10/100Base-T (Fast Ethernet)	
MC/ServiceGuard support	• Automatic switch-over to a second LAN path if the first LAN path fails. • High-availability LAN access to HP-UX Enterprise Servers means increased satisfaction and fewer calls to IT management.
Auto-Port Aggregation	• Extends existing Ethernet links into larger bandwidth pipes.
Sustains greater than 80 Mbps with 100Base-T	• Faster Internet, Intranet, data, file, and application access, especially for multimedia and high-end applications, increases end-user productivity and satisfaction.
Auto-sensing of maximum line speed on 10/100Base-T adapters	• Immediate connection to existing 10Mbps links. • Easy migration from 10Mbps Ethernet to 100Mbps Fast Ethernet. • Easy connection of 100Base-T sub-networks to existing 10Mbps Ethernet networks, using 10/100Mbps Ethernet switch.
SNMP support	• Enables remote management.
STM - Support Tools Manager (Exerciser and Verifier)	• Easier, faster management of network testing, exercise, and verification.
Dual Ultra2 SCSI	
Ultra2 LVD SCSI	• Leading edge of performance and reliability.
Up to 80 MB/s max burst rate	• High speed data transfer rates means faster access to data and files. • Faster database queries and accesses. • Faster backup.
SCSI Mirroring support	SCSI Mirroring support
Multimode LVD (Low Voltage Differential) and SE (Single Ended)	• Backwards compatibility to SE enables easy integration with existing environment.
Long cable lengths	• Up to 12 meters with LVD. Increased cable length provides greater flexibility in system configuration, especially in clustering and RAID applications.
Up to 15 devices in a daisy chain fashion	• Meets need for large disk arrays.

ordering information

A5838A	HP 2-Port 100Base-T / 2-Port Ultra2 SCSI Adapter
Option #0D1	Factory Integration
Option #AVN	Release Notes

ordering notes:

ECT 5064 Paula CPL - AC

Supported platforms (max units): Superdome (32), rp8400 (16), rp7410 (15), rp7400 (12), rp5400 series (6), rp2400 series (2). Connects to LVD or SE SCSI peripherals and 10/100BT Ethernet. Requires a SCSI terminator, not included. The terminator attaches to the last device in the SCSI chain. Order the appropriate terminator for that device. For High Density (HD) 68-pin LVD or SE: Order C2364A, for Very High Density (VHDCI) 68-pin LVD or SE: Order C2370A.

restrictions and limitations

- HVD (High Voltage Differential) devices not supported.
- 100Base-FX, 100VG-AnyLAN not supported.
- Internal SCSI connectors not supported.

for more information For additional information on this or other HP enterprise networking solutions, please visit us on the Web at unix server connectivity section, or contact any of our worldwide sales offices or HP Channel Partners. (In the U.S., call 1 800 637 7740.)

Technical information contained in this document is subject to change without notice. Performance information is estimated. Actual performance will depend on configuration.
© Copyright Hewlett-Packard Company 2000. All Rights Reserved. Reproduction, adaptation, or translation without prior written permission is prohibited except as allowed under copyright laws.
HP product information and technical documentation is available online. In addition, configuration tools and pricing information allow registered users to place orders online.

privacy statement using this site means you accept its terms

© 1994-2003 Hewlett-Packard Company

RQS Nº 03/2005 - CN
CPMI - CORREIOS
7/21/2005
Fls: 1415
Doc: 3701

Apêndice DI

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1416
Doc: 3701

hp server connectivity

tachlite fibre channel adapters

ECT
3063 Paula
CPL - AC

invent

hp enhances lineup of fibre channel adapters

hp tachlite fibre channel adapters now offer double the performance

It is truly the Information Age. Nothing but the best information management is acceptable for system-wide success. While many think computers process data into information, computers actually spend much more of their time organizing the data and managing the storage of information. This reality has been forming over time, but certainly graphical user interface programs have accelerated the trend, along with web page types of applications.

The early 1990s first saw massive disk farms created specifically to store data in very large disk arrays. Designers of storage systems quickly realized that centralized storage and retrieval of data makes information technology (IT) much more manageable. After all, when even the data that drives a meager spreadsheet on a desktop may be the decision maker for the next corporate merger or venture, it is quickly apparent that this data is too important to trust individuals to back it up regularly.

Storage area networks (SANs) are an emerging methodology for maintaining enterprise-level quantities of data. Data storage management, data integrity, cross-systems storage—all can be ensured by the use of a SAN, while they also ensure data retrieval and storage is quick and transparent to the end user. The appropriate architecture for connecting these gigantic arrays of disks becomes an important part of the decision of how to implement SANs.

benefits of hp tachlite fibre channel host bus adapters (HBAs)

- maximum I/O performance
  - auto-negotiates 2Gb or 1Gb transfer rates (A6795A only)
- superior quality with next-generation functionality:
  - switched fabric capability enabled—supports sophisticated recovery and backup scenarios, eventually without server intervention
  - online add/replace (OLAR) capable
  - increased performance with 66% less CPU utilization for I/O operations
  - full switched fabric support on HP-UX, up to 14 million nodes on a SAN
  - existing Arbitrated Loop supported
- one-stop shopping through HP for SANs, with full support for mission-critical environments

selecting your tachlite fibre channel HBA

- A6795A—PCI 2Gb Fibre Channel adapter
  - Superdome, rp8400, rp7410, rp7400, rp5400 series, rp2400 series
- A5158A—PCI 1Gb Fibre Channel adapter
  - V-class, Itanium™
  - legacy adapter for PCI-based systems
- A6685A—HSC 1Gb Fibre Channel adapter
  - K-class
- A6684A—HSC-eff 1Gb Fibre Channel adapter
  - D-class, R-class

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1417
Fls: 3701
Doc:

fibre channel provides for SAN implementations

The eventual promise of SAN technology is that regardless of where the data originates (Internet or intranet) or where it is processed (on UNIX® or Windows NT® or other operating systems), the economies of scale, ease of operations, data integrity, and performance characteristics of SANs makes them appropriate data storage/delivery architectures.

Therefore, the demand for Storage Area Networks is exploding. Through centralization, tradeoffs are made between ease of management and assurance of recovery, and, for example, more complex SAN wiring topologies.

Storage Area Networks offer flexible pools of secure storage, 100% data availability, and practically infinite scalability.

HP is committed to providing strategic technology for mass storage interconnects to its enterprise customers. For example, HP's Switched Fabric functionality allows up to 14 million nodes to be connected on a SAN. The technology usually chosen to deploy in SAN environments is Fibre Channel, which provides optimum levels of reliability, speed, and distance.

HP's Fibre Channel solution uses a standard SCSI protocol to provide a fast, robust connection to storage devices.

improved performance and investment protection

The HP PCI 2Gb Fibre Channel adapter—A6795A, available on HP-UX 11.0 and later operating systems—for Superdome, rp8400, rp7410, rp7400, rp5400 series, and rp2400 series systems, improves SAN performance and efficiency.

This adapter, also known as Tachlite, enhances HP servers' capabilities in the Storage Area Network. First, the A6795A offers data transfer rates up to 400 megabytes per second (full-duplex), effectively doubling performance over previous-generation Fibre Channel adapters. Next, the 2Gb Fibre Channel adapter auto-negotiates 1Gb or 2Gb transfer rates. This feature allows full legacy support for 1Gb SAN infrastructures, thus protecting your current SAN investment.

optimizes functionality

With all Tachlite adapters, HP delivers Switched Fabric Fibre Channel (FC-SW) functionality to HP-UX. The switched fabric functionality allows HP-UX servers to conveniently participate as a node in SAN environments.

The FC-SW functionality of Tachlite is supported on all current and future PCI platforms and offers the significant benefit of allowing servers to boot across switches. This FC-SW functionality is supported on the HP Surestore Director FC-64, FC switches 6164, 16B, and 8B, Brocade Switch 2800 and 2400, and EMC Connectrix switches.

Tachlite dramatically increases HP servers' SAN performance, resulting in 66% lower CPU utilization during I/O cycles. The new interface offers full support for peripherals and online add/replace (OLAR) in supported versions of the operating system.

HSC (K-, D-, and R-class) Switched Fabric Fibre Channel support is also available with A6685A and A6684A Tachlite adapters.

For more information, please visit the HP Web site:
www.hp.com/go/hp9000io

ECT
506
Paula
CPL - AC

tachlite features and benefits

features	benefits
2Gb and 1Gb Fibre Channel technology	• highest I/O performance for faster accessibility of databases and media-rich data • increased performance over previous-generation Fibre Channel adapters
full switched fabric Fibre Channel (FC-SW) capability	• support for sophisticated storage area network (SAN) configurations • increases scalability of SAN infrastructure up to 14 million nodes • customization of complex recovery and backup scenarios
online add/replace (OLAR)	• maximizes server uptime with OLAR • no need to bring down server to add new or replace failed adapter
arbitrated loop support	• flexibility to integrate into various SAN configurations
less CPU usage	• minimizes requirements of CPU utilization for I/O to allow for maximum cycles for other operations

product description

product number	A6795A	A5158A	A6685A	A6684A
description	**PCI 2Gb Tachlite Fibre Channel Adapter**	**PCI Tachlite Fibre Channel Adapter**	**HSC Tachlite Fibre Channel Adapter**	**HSC eff Tachlite Fibre Channel Adapter**
form factor	• standard PCI • 64-bit PCI interface, compliant with PCI Specification v2.1 • compotible with 3.3V and 5V, 32-bit and 64-bit • L=6.6 in (168 mm) W=3.5 in (89 mm) H=0.7 in (20 mm)	• standard PCI • 64-bit PCI interface, compliant with PCI Specification v2.1 • compatible with 3.3V and 5V, 32-bit and 64-bit • L=6.5 in (165 mm) W=4.7 in (120 mm) H=0.7 in (19 mm)	• HP-HSC (3x5) • HSC support (32-bit 40MHz) • L=5.7 in (145 mm) W=3.2 in (82 mm) H=1.0 in (26 mm)	• HSC EISA form factor • HSC support (32-bit 40MHz) • L=6.6 in (168 mm) W=4.2 in (107 mm) H=0.8 in (20 mm)
transfer rate	2Gb or 1Gb auto-negotiates	1Gb	1Gb	1Gb
max transfer rate	400 MB/s full duplex 200 MB/s half duplex	200 MB/s full duplex 100 MB/s half duplex	200 MB/s full duplex 100 MB/s half duplex	200 MB/s full duplex 100 MB/s half duplex
systems supported (maximum adapters)	Superdome (96) rp8400 (16) rp7410 (12) rp7400 (12) rp5400 series (10) rp2400 series (4)	Superdome (96) V-class (20) N-class (12) L-class (10) A500 (4)/A400 (2) rx9610 (16) Itanium rx4610 (10) Itanium	K-class (3–9) Kx70/Kx80 Kx60 Kx50 Kx20	D-class (3) R-class (3) Dx70/Dx80/D390 Dx20/Dx30 R380/R390
boot support	yes	yes	Kx70/Kx80 Kx60	D390 R390
operating systems	HP-UX 11.0 and later	HP-UX 11.0 and later	HP-UX 11i, 11.0, 10.20	HP-UX 11i, 11.0, 10.20
connector type	LC (SFF)	SC	SC	SC
dc power characteristics	draws 1.8 amps @ 5V	draws 1.8 amps @ 5V	draws 1.8 amps @ 5V	draws 1.8 amps @ 5V

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1418
Fls:
Doc: 3781

hp server connectivity

tachlite fibre channel adapters

environmental and regulatory specifications

product number	A6795A	A5158A	A6685A	A6684A
temperature	• non-operating: -40° to +70° C (-40° to 158° F) • operating: +5° to +40° C (41° to 104° F) • recommended operating: +20° to +30° C	• non-operating: -40° to +70° C (-40° to 158° F) • operating: +5° to +40° C (41° to 104° F) • recommended operating: +20° to +30° C	• non-operating: -40° to +70° C (-40° to 158° F) • operating: +5° to +40° C (41° to 104° F) • recommended operating: +20° to +30° C	• non-operating: -40° to +70° C (-40° to 158° F) • operating: +5° to +40° C (41° to 104° F) • recommended operating: +20° to +30° C
humidity	• operating humidity range @ 22° C: 15% to 80% RH • recommended operating: 15% to 80% RH at 22° C (70° F)	• operating humidity range @ 22° C: 15% to 80% RH • recommended operating: 15% to 80% RH at 22° C (70° F)	• operating humidity range @ 22° C: 15% to 80% RH • recommended operating: 15% to 80% RH at 22° C (70° F)	• operating humidity range @ 22° C: 15% to 80% RH • recommended operating: 15% to 80% RH at 22° C (70° F)
altitude	• non-operating: 15,000 ft • operating: 10,000 ft (3.1 km)	• non-operating: 15,000 ft • operating: 10,000 ft (3.1 km)	• non-operating: 15,000 ft • operating: 10,000 ft (3.1 km)	• non-operating: 15,000 ft • operating: 10,000 ft (3.1 km)
radiated field immunity	• EN 55022 Class A	• EN 55022 Class A	• EN 55022 Class A	• EN 55022 Class A

ordering information

product number	A6795A	A5158A	A6685A	A6684A
factory integration	• Option #0D1	• Option #0D1	• Option #0D1	• Option #0D1
release notes	• Option #AVN	• Option #AVN	• Option #AVN	• Option #AVN

for more information

For additional information on this or other HP enterprise connectivity solutions, please visit us on the Web at **www.hp.com/go/hp9000io**, or contact any of our worldwide sales offices or HP Channel Partners. (In the U.S., call 1 800 637 7740.)

Itanium is a trademark or registered trademark of Intel Corporation in the U.S. and other countries and is used under license. UNIX is a registered trademark of The Open Group. Windows NT is a U.S. registered trademark of Microsoft Corporation.

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

© Copyright Hewlett-Packard Company 2001.

05/02

5980-9011EN Rev. 1

Apêndice DJ

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1419
Doc: 3701

hp server connectivity

Gigabit Ethernet LAN

ECT
5059
Paula
CPL - AC

hp invent

comprehensive networking tools for the most demanding mission-critical and enterprise needs

hp Gigabit Ethernet LAN adapters—Gigabit performance at affordable costs

The demand for higher-speed network connections is growing at a tremendous rate in order to keep poce with the speed requirements of applications such as SAP R/3, database backups, medical, CAD/CAM, 3D modeling, animation, video, and more.

Internet data centers process terabytes of data daily. Processing, sharing, and distributing this data requires faster and faster networks.

Intelligent adapters, which take on more of the network processing from the server, are becoming critically important in helping servers cope with the onslaught of traffic running at Gigabit/second speeds. To maximize server CPU efficiency for an effective Gigabit Ethernet implementation, adapters should not only perform TCP/IP checksum, interrupt coalescing, and byte swapping, but also enable the reduction of host data copy operations.

The HP Gigabit Ethernet LAN solutions perform all of these functions and fully support the IEEE 802.3ab and 802.3z standards for Gigabit operations. These high-performance, standards-based, scalable network links allow customers to move large amounts of data quickly while leveraging their existing investments in Ethernet technology.

The HP Gigabit LAN adapters provide 1000 Mbps bandwidth over existing copper wire and fiber-optic cables, meeting the demands of e-commerce and data-intensive businesses that want to preserve their investment in existing Ethernet infrastructures. The 1000Base-T LAN adapter supports bath the CAT 5 and CAT 5e (enhanced) cabling standards. This allows superior investment protection in the existing cabling infrostructure.

The 1000Base-T adapter automatically detects the speed of the associated device as 10-, 100-, or 1000Base-T so it may be deployed immediately in any Ethernet environment. All the Gigabit LAN adapters are based on the same Ethernet standards already widely deployed in the marketplace, and they allow migration from 10 Mbps to 100 Mbps to 1000 Mbps quickly and easily, with fast deployment and minimal training needed.

The Gigabit LAN adapters are also supported with HP Auto Port Aggregation (APA) software, J4240AA. Up to 4 Gigabit Ethernet links can be logically aggregated together to form a single, extremely high-bandwidth channel with one IP address, automatic link failover, and load balancing.

In addition, HP Gigabit Ethernet adapters support HP-UX VLANs (virtual LANs). This solution offers IT managers a powerful tool that simplifies the tasks of building, managing, and securing complex network infrastructures. Physical LANs can be segmented into smaller logical or "virtual" LANS, allowing broadcast traffic to be reduced, thereby improving overall network performance. Now a change to network topology no longer requires those dreaded trips to the wiring closet!

HP-UX VLAN is compliant with host-based IEEE 802.1Q VLAN tagging, IEEE 802.1p (later incorporated in IEEE 802.1D) priority encoding, and IP Type of Service (ToS)-802.1p priority conversion.

Other key features of HP-UX VLAN include:

- IP subnet-based, protocol-based, and port-based VLAN support
- supported on HP-UX 11i v1
- configuration using well-known HP-UX tools—*lanadmin* (CLI) and SAM (GUI)
- 1024 VLANs per NIC port
- designed to work seamlessly with HP high-ovailability products, such as MC/Serviceguard
- no changes to applications required
- preserve VLAN configuration across reboot

If you would like more information regarding HP-UX VLAN functionality, please refer to the "Planning and Implementing VLANs with HP-UX" white paper, located at **www.hp.com/go/vlan**.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1420
Fls: 1
3701
Doc:

customer benefits

- increase network performance—1000 Mbps
- lower networking management costs
- leverage existing Ethernet infrastructures—including widely deployed CAT 5 cabling for 1000Base-T
- maximize CPU efficiency, thus lowering total cost of ownership
- SNMP (MIB-II) support

application areas

- Web-based Internet/intranet information distribution and transaction processing require both fast response times and high availability
- high productivity client/server systems require high-bandwidth, high-availability paths between the client, server, and data
- networking backbones—Gigabit aggregates 10/100Base-T traffic; the Gigabit links can also be aggregated with HP Auto Port Aggregation (APA) to create multi-Gigabit, high-bandwidth backbanes
- database backup demands very high bandwidth and availability to ensure one-pass backup
- solutions requiring high-performance connections for voice, video, streaming, multimedia, and high-end applications
- network-attached storage

features and benefits

features	benefits
1000 Mbps (Gigabit speed)	• high-performance, high-bandwidth Gigabit networking—1000 Mbps • ideal for media-rich data, Internet applications, and high-speed data centers • faster network backups and data access
1000Base-T and 1000Base-SX Ethernet standards (IEEE 802.3ab and IEEE 802.3z)	• seamlessly integrates into existing Ethernet infrastructures • lower cost to implement and manage • leverage current investments in Ethernet and cable infrastructure
auto-negotiation: tri-speed—10, 100, or 1000 Mbps for the 1000Base-T adapter	• flexible, easy to deploy • odopts for growing network bandwidth requirements
CPU offlood (Internet checksum offload, byte swapping, interrupt coalescence and ovoidance)	• increases performance • maximizes server CPU efficiency
HP-UX VLAN (virtual LAN)	• enables logical connectivity separation of a network from physical connectivity • isolates traffic and preserves bondwidth • improves network manogeability and performance
MC/Serviceguard (MCSG) and Auto Port Aggregation (APA) support	• MCSG offers highest levels of high availability • APA can aggregate up to 4 Gigabit links to create a "super" bandwidth connection
Online Addition and Replacement (OLAR)	• server uptime is maximized, since adapters con be added or replaced without the need to bring the system down
up to 550-meter cabling lengths (dependent on cable) for the 1000Base-SX adapter	• ultimate flexibility in data center layouts, backbone implementations, or high-performance client networks
dual DMA channels for simultaneous read ond write; embedded RISC processor	• enhanced performance for every type of networking task—downloading, uploading, file transfers, and intense bi-directional traffic

next-generation Gigabit Ethernet specifications

product number	A6825A	A6847A
description	PCI HP-UX 1000Base-T Gigabit Ethernet Adapter	PCI HP-UX 1000Base-SX Gigabit Ethernet Adapter
systems supported	rp2400 series rx2600 series rp5400 series rx5600 series rp7400 series rp8400 superdome	rp2400 series rx2600 series rp5400 series rx5600 series rp7400 series rp8400 superdome
maximum number of active cards	rp2400 series: 4 rx2600 series: 4 rp5400 series: 10 rx5600 series: 9 rp7400: 12 rp7410: 15 rp8400: 16 superdome: 16, 32, or 64 (depends on configuration)	rp2400 series: 4 rx2600 series: 4 rp5400 series: 10 rx5600 series: 9 rp7400: 12 rp7410: 15 rp8400: 16 superdome: 16, 32, or 64 (depends on configuration)
release(s) supported	HP-UX 11.0, 11i v1, and 11i v1.6	HP-UX 11.0, 11i v1, and 11i v1.6
VLAN supported	yes (for 11i v1 only)	yes (for 11i v1 only)
OLAR support	yes (for 11i v1 only)	yes (for 11i v1 only)
connector type	RJ-45	duplex SC
cabling	CAT 5, CAT 5e e CAT 6 unshielded twisted pair (UTP) copper cabling	multi-mode fiber (62.5 or 50 micron)
wavelength	NA	850 nm
CPU offload features	yes	yes
auto-sensing speed	10, 100, 1000 Mbps	1000 Mbps only
auto-negotiation	yes	yes
duplex support	full duplex for 10/100/1000 Mbps half duplex for 10/100 Mbps	full duplex for 1000 Mbps half duplex not supported for fiber
jumbo frame support	yes (at 1000 Mbps only)	yes
MC/Serviceguard support	yes	yes
Auto Port Aggregation support	yes (for 11i v1 only)	yes (for 11i v1 only)
operating distance	up to 100 meters	up to 550 meters (dependent on cable)
Ethernet standard	IEEE 802.3ab IEEE 802.3u	IEEE 802.3z
form factor/host bus	64-bit/66 MHz PCI	64-bit/66 MHz PCI
card size	2.536 x 6.6 in (64.4 x 167.6 mm)	2.536 x 6.6 in (64.4 x 167.6 mm)

ECT 5057 Paula AC
CPMI - CORREIOS
1421
Fls: 3
Doc:

additional hp-ux Gigabit Ethernet features and specifications

feature	all hp-ux Gigabit Ethernet LAN adapters
NIC to NIC connection	yes
link level and IP multi-cost support	yes
promiscuous mode (link and SAP)	yes
SNMP (MIB-II) support	yes
activity and status LED indicators	yes
universal keyed, 3.3 and 5v tolerant	yes (for PCI cards only)
SAM configurable	yes
protocols	TCP/IP, UDP/IP, NFS
customer installable	yes (except on Superdome)
hp MAC address	yes

operating distance for 1000Base-SX

1000Base-SX (850 nm SWL)	modal bandwidth (classification of fiber-optic cable)	operating distance
62.5-micron MMF cable	160 (MHz x km) 200 (MHz x km)	up to 220 meters up to 275 meters
50-micron MMF cable	400 (MHz x km) 500 (MHz x km)	up to 500 meters up to 550 meters

environmental specifications for A6825A and A6847A

temperature	non-operating: operating:	–40° to 60° C (–40° to 140° F) 0° to 50° C (32° to 122° F)
humidity	non-operating: operating:	5 to 95% RH non-condensing (20%/hour) 5 to 95% RH non-condensing at 40° C (104° F) (16-hour dwells at extremes)
altitude	non-operating: operating:	10.6 km (35,000 ft) 3.1 km (10,000 ft)
electromagnetic compatibility	USA: Europe: Australia: Japan: harmonic: flicker/fluctuation:	FCC, Class B CISPR-22/EN55022, Class B AS/NZS 3548 Class B VCCI, Class B EN61000-3-2 EN61000-3-3

next-generation Gigabit Ethernet ordering information

A6825A–1000Base-T PCI Gigabit Ethernet LAN Adapter
Option #0D1–Factory integration
Option #AVN–Release notes

A6847A–1000Base-SX PCI LAN Adapter
Option #0D1–Factory integration
Option #AVN–Release notes

for more information

For additional information on this or other HP enterprise networking solutions, please visit us on the Web at **www.hp.com/go/hp9000io**, visit our technical documentation site at **http://docs.hp.com/hpux/netcom/index.html**, or contact any of our worldwide sales offices or HP Channel Partners. In the U.S., call 1-800-637-7740.

© Copyright 2003 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice and is provided "as is" without warranty of any kind. The 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.

05/23/03
5980-7059EN, Rev. 3

Apêndice DL

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1422
Fls:
3701
Doc:

5055 Laura CPL - AC

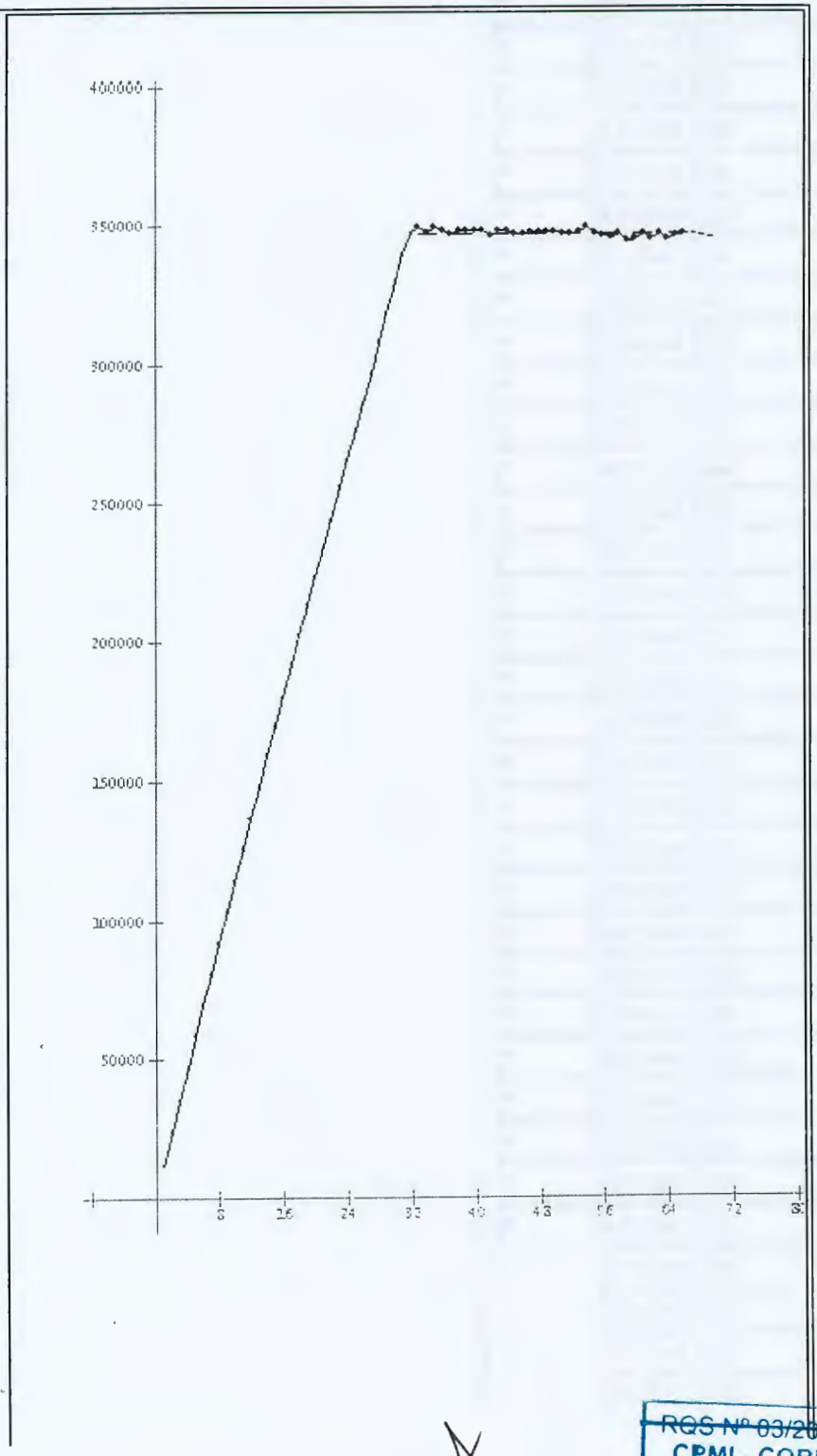
SPECjbb2000

SPECjbb2000 = 346862 ops/s

Hewlett-Packard HP Superdome Server

Hewlett-Packard Hotspot 1.4.1.02 64-bit VM on HP-UX 11i for PA-RISC 8700+

Warehouses	Ops/s	Incl. in metric
1	11373	
2	23410	
3	35111	
4	46510	
5	58126	
6	69583	
7	80849	
8	92122	
9	103517	
10	114673	
11	125960	
12	136898	
13	148008	
14	159330	
15	169946	
16	180066	
17	191437	
18	202294	
19	213113	
20	223679	
21	234384	
22	244313	
23	255572	
24	265863	
25	276975	
26	286413	
27	296516	
28	308404	
29	318573	
30	329198	
31	339563	
32	346954	



RQS Nº 03/2005 - CN
CPMI - CORREIOS
1423
Fls:
Doc: 3701

33	349338	*
34	347126	*
35	348893	*
36	348069	*
37	346529	*
38	347827	*
39	348003	*
40	348043	*
41	347853	*
42	346035	*
43	347616	*
44	347922	*
45	346819	*
46	346469	*
47	347201	*
48	347219	*
49	347320	*
50	347209	*
51	346854	*
52	346850	*
53	346987	*
54	349036	*
55	346474	*
56	346251	*
57	345192	*
58	346883	*
59	344254	*
60	344663	*
61	346493	*
62	344528	*
63	346373	*
64	344509	*
65	346130	*
66	346354	*
67	346525	
68	346134	
69	345452	
70	345704	

SPECjbb2000	**(from 33 to 66)**	**346862 ops/s**

SPEC license # 3	**Tested by:** Hewlett-Packard	**Test date:** Feb 4, 2003

Hardware	
Hardware Vendor	Hewlett-Packard
Vendor URL	http://www.hp.com
Model	HP Superdome Server
Processor	PA-RISC 8700+
MHz	875
# of Procs	32
Memory (MB)	128 GB
Primary cache	786KBI+1536KBD
Secondary cache	none
Other cache	none
Filesystem	VxFS
Disks	5 x 16 GB SCSI
Other hardware	none

Software	
Software Vendor	Hewlett-Packard
Vendor URL	http://www.hp.com
Java Precompiler Version	none
Java Precompiler Command Line	
Java Precompiler Way Of Excluding Classes	none
JVM Version	Hotspot 1.4.1.02 64-bit VM on HP-UX 11i for PA-RISC 8700+
JVM Command Line	java -XX:+ServerApp -XX:+AggressiveHeap -Xmn80g -ms82g -mx82g spec.jbb.JBBmain -propfile Test1
JVM Initial Heap Memory (MB)	82 GB
JVM Maximum Heap Memory (MB)	82 GB
JVM CLASSPATH	./jbb.jar: ./jbb_no_precompile.jar: ./check.jar: ./reporter.jar:
JVM BOOTCLASSPATH	/opt/java1.4.1/jre/lib/rt.jar: /opt/java1.4.1/jre/lib/i18n.jar: /opt/java1.4.1/jre/lib/sunrsasign.jar: /opt/java1.4.1/jre/lib/jsse.jar: /opt/java1.4.1/jre/lib/jce.jar: /opt/java1.4.1/jre/lib/charsets.jar: /opt/java1.4.1/jre/classes
OS Version	HP-UX 11i v1.0
System state	normal
Other software	none

Test Information	
Tested by	Hewlett-Packard
SPEC license #	3
Test location	Cupertino, CA

Tuning

Notes
+AggressiveHeap instructs the JVM to push memory use to the limit and sets the memory management policy to defer collection as much as possible. If you want to use different heap values, you can do so

ECT - AC - 5053 - Fls. 1424
RGS Nº 08/2005 - CN
CPMI - CORREIOS
Fls: 1424
Doc: 3701

Test date	Feb 4, 2003
H/w available	Jun-2002
JVM available	Jun-2003
OS available	Dec-2000
Other s/w available	

by setting the -Xmn, -ms, -mx options after specifying AggressiveHeap on the command line.

Details of Runs

Warehouses	Thrput	Total heap (MB)		Thread spread %	% > 120s	transaction type	Count	Time (in seconds)	
		Size	Used					total	max
1	11373	83429	35.0	<0.01%	.017	new_order	593496	68.9	.020
						payment	593499	22.7	.020
						order_status	59350	2.68	.020
						delivery	59350	8.90	.020
						stock_level	59349	9.42	.020
2	23410	83429	57.6	.523%	.025	new_order	1221685	143	.029
						payment	1221682	47.5	.029
						order_status	122169	5.38	.020
						delivery	122168	17.3	.021
						stock_level	122169	19.8	.020
3	35111	83429	78.9	.150%	.017	new_order	1832167	217	.020
						payment	1832163	70.9	.020
						order_status	183216	7.42	.020
						delivery	183217	27.9	.020
						stock_level	183218	26.9	.020
4	46510	83429	104	.776%	.017	new_order	2427042	288	.020
						payment	2427033	94.8	.020
						order_status	242701	10.1	.020
						delivery	242705	36.2	.020
						stock_level	242705	37.0	.020
5	58126	83429	125	.946%	.017	new_order	3033181	360	.020
						payment	3033179	122	.020
						order_status	303318	13.6	.020
						delivery	303318	42.8	.020
						stock_level	303320	45.5	.020
6	69583	83429	147	1.38%	.017	new_order	3631040	427	.020
						payment	3631044	147	.020

						order_status	363104	16.2	.020
						delivery	363106	54.9	.020
						stock_level	363104	54.6	.020
7	80849	83429	169	1.19%	<0.01	new_order	4218584	497	.029
						payment	4218572	168	.029
						order_status	421860	19.1	.029
						delivery	421857	63.2	.029
						stock_level	421857	68.1	.029
8	92122	83429	192	.665%	.017	new_order	4807166	573	.020
						payment	4807155	194	.020
						order_status	480715	20.8	.020
						delivery	480714	72.3	.020
						stock_level	480717	74.9	.020
9	103517	83429	218	1.16%	.025	new_order	5402214	641	.029
						payment	5402220	216	.029
						order_status	540221	24.0	.029
						delivery	540222	84.0	.029
						stock_level	540221	85.0	.020
10	114673	83429	236	1.43%	.025	new_order	5984421	712	.030
						payment	5984432	244	.028
						order_status	598442	26.8	.030
						delivery	598443	90.6	.030
						stock_level	598441	93.1	.030
11	125960	83429	260	1.44%	.017	new_order	6572931	787	.028
						payment	6572953	269	.028
						order_status	657296	29.2	.028
						delivery	657293	99.0	.028
						stock_level	657297	101	.028
12	136898	83429	283	1.46%	.017	new_order	7143684	850	.030
						payment	7143682	292	.030
						order_status	714364	33.9	.020
						delivery	714367	110	.020
						stock_level	714367	116	.030
13	148008	83429	306	1.44%	.017	new_order	7723468	924	.029
						payment	7723460	314	.029
						order_status	772346	33.7	.021
						delivery	772347	123	.029
						stock_level	772348	123	.029

ECT 5051 Fls: 1 - AC

RQS N° 03/2005 - CN
CPMI - CORREIOS
6/29/2005
Fls: 1425
Doc: 3701

14	159330	83429	330	1.37%	.017	new_order	8314229	996	.029
						payment	8314235	341	.029
						order_status	831423	36.7	.029
						delivery	831421	129	.029
						stock_level	831422	131	.029
15	169946	83429	351	1.35%	.033	new_order	8869726	1066	.030
						payment	8869721	362	.030
						order_status	886969	41.1	.020
						delivery	886974	140	.030
						stock_level	886972	141	.030
16	180066	83429	370	1.02%	<0.01	new_order	9395518	1129	.029
						payment	9395497	387	.260
						order_status	939553	42.1	.028
						delivery	939548	154	.260
						stock_level	939552	152	.260
17	191437	83429	392	1.06%	.017	new_order	9989675	1203	.260
						payment	9989679	414	.260
						order_status	998962	47.2	.020
						delivery	998969	158	.260
						stock_level	998963	159	.020
18	202294	83429	418	1.30%	.017	new_order	10556241	1275	.260
						payment	10556251	439	.260
						order_status	1055632	48.2	.260
						delivery	1055624	169	.030
						stock_level	1055627	165	.030
19	213113	83429	436	1.04%	<0.01	new_order	11119841	1353	.240
						payment	11119855	453	.240
						order_status	1111981	51.9	.029
						delivery	1111984	179	.240
						stock_level	1111984	176	.240
20	223679	83429	456	1.46%	<0.01	new_order	11671187	1422	.260
						payment	11671174	483	.028
						order_status	1167116	54.8	.028
						delivery	1167115	184	.260
						stock_level	1167122	185	.260
21	234384	83429	487	1.49%	.025	new_order	12231795	1485	.290
						payment	12231794	515	.290
						order_status	1223177	56.5	.029

E C T
C/ Paulo
AC

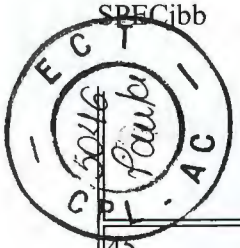
						delivery	1223183	192	.290
						stock_level	1223177	199	.030
22	244313	83429	505	1.53%	.042	new_order	12752064	1550	.280
						payment	12752062	534	.260
						order_status	1275203	59.9	.028
						delivery	1275199	207	.260
						stock_level	1275205	209	.030
23	255572	83429	533	2.33%	.025	new_order	13337542	1625	.300
						payment	13337517	560	.300
						order_status	1333759	64.2	.300
						delivery	1333749	214	.300
						stock_level	1333753	214	.030
24	265863	83429	549	1.90%	.042	new_order	13876891	1699	.300
						payment	13876888	578	.300
						order_status	1387686	64.7	.022
						delivery	1387686	225	.300
						stock_level	1387694	226	.300
25	276975	83429	572	1.26%	<0.01	new_order	14452078	1763	.300
						payment	14452096	611	.300
						order_status	1445215	69.4	.300
						delivery	1445213	231	.300
						stock_level	1445206	234	.300
26	286413	83429	595	1.50%	.017	new_order	14945793	1839	.280
						payment	14945790	635	.300
						order_status	1494578	69.9	.021
						delivery	1494579	238	.300
						stock_level	1494585	243	.022
27	296516	83429	620	1.51%	.025	new_order	15474268	1898	.300
						payment	15474262	656	.300
						order_status	1547422	74.2	.300
						delivery	1547428	253	.300
						stock_level	1547429	258	.029
28	308404	83429	639	1.93%	.025	new_order	16094681	1986	.320
						payment	16094662	678	.320
						order_status	1609472	76.2	.030
						delivery	1609464	262	.320
						stock_level	1609471	255	.030
29	318573	83429	666	1.41%	.017	new_order	16623970	2047	.320

RQS Nº 03/2005 - CN
CPMI - CORREIOS
6/29/2003
1426
Fls:
Doc: 3701

						payment	16623981	705	.320
						order_status	1662396	80.4	.030
						delivery	1662391	269	.320
						stock_level	1662399	271	.320
30	329198	83429	688	2.15%	.025	new_order	17179807	2119	.320
						payment	17179837	728	.320
						order_status	1717985	81.7	.320
						delivery	1717982	283	.030
						stock_level	1717978	276	.030
31	339563	83429	711	1.57%	.025	new_order	17720745	2197	.340
						payment	17720723	751	.340
						order_status	1772081	81.9	.030
						delivery	1772075	288	.340
						stock_level	1772071	286	.030
32	346954	83429	737	2.23%	.042	new_order	18109505	2251	.860
						payment	18109478	774	.860
						order_status	1810953	88.7	.610
						delivery	1810945	305	.860
						stock_level	1810954	299	.860
33	349338	83429	748	13.6%	.025	new_order	18230885	2312	1.01
						payment	18230878	806	1.08
						order_status	1823087	90.3	.800
						delivery	1823087	313	1.01
						stock_level	1823081	309	1.01
34	347126	83429	762	51.2%	.042	new_order	18118452	2379	1.13
						payment	18118464	831	.990
						order_status	1811848	93.9	.590
						delivery	1811848	321	.970
						stock_level	1811845	326	.890
35	348893	83429	789	51.8%	.025	new_order	18207687	2462	.940
						payment	18207679	844	1.37
						order_status	1820770	96.4	.600
						delivery	1820768	330	.700
						stock_level	1820768	331	.360
36	348069	83429	813	39.5%	.042	new_order	18167687	2513	1.08
						payment	18167680	885	.900
						order_status	1816771	99.9	.500
						delivery	1816768	346	1.00

						stock_level	1816771	335	.900
37	346529	83429	831	44.0%	.033	new_order	18085817	2590	1.09
						payment	18085836	909	1.02
						order_status	1808585	99.0	.760
						delivery	1808577	346	.960
						stock_level	1808583	353	.890
38	347827	83429	847	36.0%	.025	new_order	18152071	2673	1.00
						payment	18152049	923	.900
						order_status	1815206	104	.300
						delivery	1815201	359	.770
						stock_level	1815206	354	.800
39	348003	83429	877	41.9%	.017	new_order	18159697	2720	1.00
						payment	18159691	958	1.35
						order_status	1815975	107	.880
						delivery	1815972	378	.980
						stock_level	1815970	369	1.00
40	348043	83429	892	50.0%	.042	new_order	18166317	2800	1.08
						payment	18166360	973	1.00
						order_status	1816636	112	.900
						delivery	1816636	380	1.02
						stock_level	1816628	379	1.18
41	347853	83429	911	48.7%	.033	new_order	18154889	2861	1.40
						payment	18154877	1007	1.00
						order_status	1815488	112	.660
						delivery	1815484	395	.880
						stock_level	1815490	387	1.02
42	346035	83429	925	49.3%	.025	new_order	18058530	2919	1.09
						payment	18058521	1031	1.01
						order_status	1805850	116	.990
						delivery	1805845	407	1.04
						stock_level	1805851	408	1.04
43	347616	83429	941	51.3%	.033	new_order	18142511	3017	1.08
						payment	18142537	1059	1.00
						order_status	1814251	119	.500
						delivery	1814250	403	.800
						stock_level	1814255	405	1.00
44	347922	83429	966	47.5%	.058	new_order	18163045	3075	1.21
						payment	18163054	1071	1.08

RQS Nº 03/2005 - CN
CPMI - CORREIOS
6/29/2003
Fls: 1427
Doc: 3701



						order_status	1816310	123	1.00
						delivery	1816309	428	1.11
						stock_level	1816305	416	1.01
45	346819	83429	987	42.4%	.042	new_order	18102457	3157	1.13
						payment	18102462	1105	1.01
						order_status	1810241	126	1.11
						delivery	1810240	430	1.11
						stock_level	1810245	415	1.07
46	346469	83429	1010	46.4%	.042	new_order	18084153	3222	1.02
						payment	18084153	1117	1.07
						order_status	1808416	130	.900
						delivery	1808412	444	1.04
						stock_level	1808415	429	1.02
47	347201	83429	1025	47.8%	.033	new_order	18120893	3269	1.99
						payment	18120906	1154	1.99
						order_status	1812090	124	.820
						delivery	1812091	464	1.10
						stock_level	1812084	455	1.99
48	347219	83429	1048	45.8%	.033	new_order	18121791	3345	1.09
						payment	18121822	1163	1.09
						order_status	1812179	135	1.03
						delivery	1812187	466	1.13
						stock_level	1812186	455	1.09
49	347320	83429	1070	44.9%	.033	new_order	18127083	3420	1.60
						payment	18127094	1195	1.10
						order_status	1812711	131	.311
						delivery	1812705	481	2.50
						stock_level	1812702	464	1.02
50	347209	83429	1084	42.5%	.042	new_order	18122815	3493	1.77
						payment	18122775	1213	1.69
						order_status	1812275	143	1.11
						delivery	1812283	489	1.69
						stock_level	1812283	476	1.69
51	346854	83429	1105	40.6%	.025	new_order	18101260	3587	2.85
						payment	18101278	1220	1.91
						order_status	1810129	144	.900
						delivery	1810123	499	1.99
						stock_level	1810123	472	1.40

ECT 5045 Paula L - AC

52	346850	83429	1127	44.7%	.033	new_order	18102561	3626	1.71
						payment	18102567	1254	1.81
						order_status	1810253	145	1.08
						delivery	1810256	526	1.71
						stock_level	1810257	485	.999
53	346987	83429	1150	39.7%	.042	new_order	18111240	3690	2.00
						payment	18111218	1286	2.00
						order_status	1811125	140	1.10
						delivery	1811117	542	1.90
						stock_level	1811117	501	1.91
54	349036	83429	1161	36.8%	<0.01	new_order	18119506	3730	2.00
						payment	18119528	1293	1.90
						order_status	1811948	143	1.20
						delivery	1811943	549	1.96
						stock_level	1811954	518	1.90
55	346474	83429	1186	40.5%	.150	new_order	18104033	3840	2.08
						payment	18104001	1340	1.49
						order_status	1810402	151	1.10
						delivery	1810400	543	1.89
						stock_level	1810401	522	1.49
56	346251	83429	1206	40.9%	.025	new_order	18069769	3883	2.29
						payment	18069759	1359	1.99
						order_status	1806978	159	1.49
						delivery	1806975	567	2.09
						stock_level	1806972	529	1.99
57	345192	83429	1217	30.2%	.033	new_order	18016031	3953	2.10
						payment	18016032	1381	1.99
						order_status	1801600	164	1.70
						delivery	1801600	587	2.33
						stock_level	1801597	533	2.10
58	346883	83429	1238	43.1%	.033	new_order	18104299	4006	2.00
						payment	18104294	1422	2.99
						order_status	1810427	162	2.95
						delivery	1810434	584	2.00
						stock_level	1810427	535	1.33
59	344254	83429	1259	35.5%	.042	new_order	17968548	4092	1.80
						payment	17968553	1443	1.80
						order_status	1796853	164	1.78

RQS Nº 03/2005 - CN CPMI - CORREIOS
Fls: 1428
3701
Doc:

						delivery	1796856	593	2.84
						stock_level	1796859	555	1.50
60	344663	83429	1275	38.6%	.033	new_order	17988404	4151	2.01
						payment	17988433	1442	2.00
						order_status	1798839	162	1.90
						delivery	1798839	645	2.00
						stock_level	1798848	573	2.00
61	346493	83429	1299	33.8%	.033	new_order	18083923	4169	2.00
						payment	18083901	1496	2.00
						order_status	1808392	169	1.60
						delivery	1808388	679	2.30
						stock_level	1808388	574	1.98
62	344528	83429	1313	37.1%	.025	new_order	17979884	4247	2.20
						payment	17979862	1505	2.41
						order_status	1797987	170	1.98
						delivery	1797982	652	2.00
						stock_level	1797976	609	2.10
63	346373	83429	1340	25.9%	.033	new_order	18077670	4338	2.05
						payment	18077652	1517	1.99
						order_status	1807756	169	1.69
						delivery	1807771	681	2.09
						stock_level	1807760	613	1.89
64	344509	83429	1354	39.1%	.025	new_order	17978875	4420	2.23
						payment	17978881	1560	2.58
						order_status	1797889	185	1.90
						delivery	1797882	663	2.08
						stock_level	1797887	618	2.00
65	346130	83429	1377	44.5%	.050	new_order	18067991	4451	2.53
						payment	18068003	1606	2.37
						order_status	1806799	169	1.10
						delivery	1806801	682	2.41
						stock_level	1806803	621	2.08
66	346354	83429	1395	33.2%	.033	new_order	18076666	4512	2.09
						payment	18076615	1617	2.09
						order_status	1807667	171	2.51
						delivery	1807665	740	2.10
						stock_level	1807663	601	1.90
67	346525	83429	1417	38.0%	.183	new_order	18112674	4571	2.80

ECT 5043 Fls. AC

						payment	18112718	1634	2.20
						order_status	1811265	194	2.20
						delivery	1811265	753	3.40
						stock_level	1811276	625	2.18
68	346134	83429	1430	46.4%	.033	new_order	18065146	4693	2.40
						payment	18065180	1677	1.85
						order_status	1806520	191	1.35
						delivery	1806519	689	1.91
						stock_level	1806512	647	1.89
69	345452	83429	1447	31.3%	.058	new_order	18034094	4739	2.07
						payment	18034135	1675	2.17
						order_status	1803408	189	1.90
						delivery	1803409	749	2.22
						stock_level	1803414	643	2.10
70	345704	83429	1472	27.7%	.042	new_order	18044214	4799	2.71
						payment	18044235	1720	2.60
						order_status	1804421	200	1.80
						delivery	1804422	804	2.40
						stock_level	1804420	626	1.70

SPECjbb2000 Version: [SPECjbb2000 1.02, December 14, 2001]

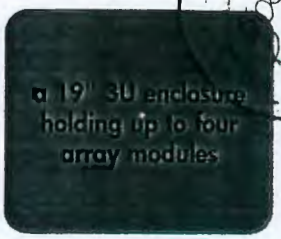
Reporting page, Copyright © 2000-2002 SPEC. All rights reserved

RQS Nº 03/2005 - CN
CPMI - CORREIOS
6/29/2003
Fls: 1429
Doc: 3701

Apêndice DM

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1430
Doc: 3701

hp invent



The HP Surestore Tape Array 5300 is a 3U rack enclosure that will hold two full-height array modules, four half-height modules, or one full-height and two half-height modules. The enclosure supports HP array modules, including Ultrium 230, Ultrium 215, DLT 80, DLT vs80, DAT 40 (DDS-4), and DAT 24 (DDS-3) tape drives, plus a DVD-ROM. The wide variety and interchangeability of array modules provides a truly flexible solution for use in a variety of different data storage situations.

For IT managers whose environments require added data security and accessibility, the Tape Array 5300 also has an optional upgrade kit—the PSU/fan kit provides a redundant fan and power supply.

key features and benefits

- **expandable:** holds up to four offline hot-swappable array modules on four independent SCSI buses
- **upgradable:** allows you to expand from one to four tape drives as your capacity requirements grow
- **flexible:** supports HP array modules: Ultrium 230, Ultrium 215, DLT 80, DLT vs80, DAT 40 (DDS-4), DAT 24 (DDS-3) and DVD-ROM
- **compact:** stores 800 GB of compressed data per array with four Ultrium 215 drives in 3U of rack space
- **high availability:** maximizes system uptime and performance with optional redundant components
- **rackable:** fits in standard 19" racks from HP, Apex, and Rittal

tape drive comparison

model	form factor	capacity*	performance*
DAT 24m	Half-height	24 GB	7.2 GB/hour
DAT 40m	Half-height	40 GB	21.6 GB/hour
DLT vs80m	Half-height	80 GB	21.6 GB/hour
DLT 80m**	Full-height	80 GB	43.2 GB/hour
Ultrium 215m	Half-height	200 GB	54 GB/hour
Ultrium 230m**	Full-height	200 GB	108 GB/hour

*Capacity and performance are based on 2:1 data compression. Actual compression varies with data type.
** These modules are also compatible with Tape Array 5500.

ECT - AC
RQS Nº 03/2005 - CN
CPMI - CORREIOS
1431
Fls:
3701
Doc:

invent

technical specifications

dimensions (h x w x d)	741 x 445 x 133 mm (29.2 x 17.5 x 5.25 in)
weight	13 kg (28.71 lb)
native capacity	400 GB with four Ultrium 215 drives
compressed capacity	800 GB* with four Ultrium 215 drives
external I/O ports	Eight SCSI ports (one in and one out per half-height drive bay)
power supply/ required	100–127V AC (+/–10%) or 200–240V AC (+/–10%)
operating temperature range	5° to 40°C (41° to 104°F)
storage temperature range	–40° to 70°C (–40° to 158°F)
operating humidity range	20% to 80% RH
non-operating humidity	5% to 95% RH

*Capacities and transfer rates assume 2:1 data compression. Actual compression moy differ because compression varies with data type.

ordering information

C7508A	Tape Array 5300	Four-bay rack enclosure
C7496A	Tape Array PSU/fan kit	Redundant power supply and fan
compatible array modules		
C7456A	DLT 80m	DLT 80 array module (full-height)
C7507A	DLT vs80m	DLT vs80 array module (half-height)
C7470A	Ultrium 230m	Ultrium 230 array module (full-height)
C7492A	Ultrium 215m	Ultrium 215 array module (half-height)
C7497A	DAT 40m	DAT 40 array module (half-height)
C7498A	DAT 24m	DAT 24 array module (half-height)
C7499A	DVD-ROM	DVD-ROM array module (half-height)

additional information

target use
Providing a scalable, flexible means of racking standalone products or adding versatile storage capability to a local area network

target audience
IT managers of mid-sized companies who have a rack environment and require a scalable backup solution that supports a variety of tape technologies and DVD-ROM for software loading

what's in the box
Enclosure, mounting rails, rack-mounting kit (for HP & other racks), rack-mounting template, manuals, Surestore CD containing documentation, power cord, power supply unit (PSU), PSU bay filler panel, fan, fan bay filler panel, torx tool, drive bay filler panels, accessory kit

warranty features—hp service and support
3-year, next-day onsite response; system matching on HP rack servers

warranty options
H4618A / H4618E 3-year, same-day, onsite

for more information

For more information on HP storage products, contact any of our worldwide sales offices or visit our Web site at: **www.hp.com/go/storage**

Windows is a U.S. registered trademark of Microsoft Corporation.
Technical information in this document is subject to change without notice.
©Hewlett-Packard Company 2001
11/01
5980-8611EN

Apêndice DN

ROS Nº 03/2005 - CN
CPMI - CORREIOS
1433
Fls: 3701
Doc:

CPL - AC
São Paulo

↑ HP C/HP-UX Reference Manual
↑ What is HP C?
← Compatibility Mode

HP C Online Help →

About HP C/HP-UX

This manual presents ANSI C as the standard version of the C language. Where certain constructs are not available in compatibility mode, or would work differently, it is noted and the differences are described.

HP C/HP-UX, when invoked in ANSI mode, is a conforming implementation of ANSI C, as specified by American National Standard 9899-1990. This manual uses the terminology of that standard and attempts to explain the language defined by that standard, while also documenting the implementation decisions and extensions made in HP C/HP-UX. It is not the intent of this document to replicate the standard. Thus, you are encouraged to refer to the ndard for any fine points of the language not covered here.

← Compatibility Mode

HP C Online Help →

RQS Nº 03/2005 - CN
CPMI - CORREIOS
7/12/2005
Fls: 1434
Doc: 3791

Apêndice DO

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1435
Doc: 3791

ECT 5039 Paula AC

construindo sua infra-estrutura - sempre ativa com servidores **hp**

soluções de servidor de internet poderosas e flexíveis para uma infra-estrutura sempre ativa

hp superdome

O centro de processamento de dados da Internet é o elemento crítico que possibilitará a próxima geração dos negócios. E ao projetar e implementar sua solução de Internet, sua primeira preocupação deve ser encontrar produtos e serviços de tecnologia que sejam construídos corretamente logo na primeira vez. Sua próxima preocupação será assegurar que o que funciona hoje também vai atender as suas necessidades futuras, à medida que novas oportunidades — e novos desafios — se apresentarem.

A infra-estrutura de tecnologia correta é aquela que está sempre ativa onde e como for necessário. Isso é o que a HP pode ajudá-lo a construir — e não há precedentes na indústria.

Os servidores HP Superdome fornecem uma combinação sob medida de tecnologia e serviços. Construída com componentes-chave, tais como as habilidades comprovadas da HP em centros de processamento de dados, sua experiência em e-services e sua força em desenvolvimento de utilitários, sua infra-estrutura sempre ativa fornecerá uma experiência excepcional para os clientes, assegurando a facilidade, velocidade e eficácia.

sua infra-estrutura sempre ativa

Tratando dos inúmeros desafios difíceis que você enfrenta ao construir e gerenciar uma empresa de Internet, a HP fornece:

- HP Superdome Servidores UNIX líderes da indústria
- Blocos de construção de utilitários-somente da HP
- A mais ampla oferta de capacidades de particionamento da indústria, com o "continuum" particionamento da HP
- Itanium™ e capacidade para SOs variados

sempre presente

A HP também está sempre presente para você, desde o primeiro contato. A HP fornece:

- Gerenciamento de soluções de loop fechado
- Avaliações iniciais
- Pré-integração e testes
- Treinamento baseado em necessidades
- Serviços de migração

E asseguramos que sua infra-estrutura funcionará continuamente com:

- Serviços proativos
- Acordos para reparos

uma experiência excepcional para o cliente

A implementação bem-sucedida de um centro de processamento de dados exige muito mais do que tecnologia. É por isso que a infra-estrutura sempre ativa está sempre com você — em todas as etapas do caminho.

- **invente:** facilidade de planejamento e projeto para uma solução que é feita sob medida para se adequar imediatamente aos seus negócios
- **construa:** velocidade de integração e instalação de uma infra-estrutura pronta para funcionar
- **execute:** serviços de missão crítica e tecnologias que possibilitam uma operação contínua, uma capacidade flexível e um gerenciamento eficiente para assegurar a excelência operacional do dia-a-dia
- **evolua:** plano à prova de obsolescência, desenvolvimento de utilitários e cuidado contínuo para atender a suas necessidades por toda a vida de sua empresa

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1436
Fls: 3701
Doc:

três configurações do hp superdome para atender a suas necessidades

As implementações de grande porte em geral não correspondem às expectativas, como resultado de habilidades inadequadas que são aplicadas nas etapas de projeto e implementação. Com o Superdome, o HP garante a você uma experiência excepcional de computação, através de serviços HP líderes da indústria e parceiros de canal selecionados, disponível em três configurações pré-definidas. Para todas as configurações existem soluções de financiamento disponíveis para atender os seus requisitos orçamentários.

configuração básica

A construção da base correta reduz drasticamente os problemas e acelera o tempo de instalação em produção, de forma que todas as soluções Superdome incluirão a Configuração Básica como base para um desempenho excelente. A Configuração Básica destina-se a empresas cujos aplicativos têm requisitos de disponibilidade de baixa prioridade ou que possuem especialistas em suas equipes para executar e gerenciar seus próprios ambientes de TI.

- Gerenciamento de projetos em loop fechado utilizando metodologias baseadas em processos e medidas para assegurar seu sucesso e satisfação
- Serviços de consultoria para um projeto detalhado de arquitetura para assegurar que esteja correto logo na primeira vez
- Avaliação de habilidades e treinamento específico em Superdome para fornecer à equipe de TI as habilidades necessárias
- Preparação completa do local/ambiente para ajudá-lo a compreender e abordar as exigências de sua localização física
- Integração e testes de fábrica da HP para assegurar que o sistema esteja adequadamente configurado e chegue pronto para funcionar
- Suporte contínuo de centro de respostas, disponível 24 horas por dia, 7 dias por semana, com compromisso de resposta em 4 horas

configuração de sistemas críticos

Para um alto nível de disponibilidade de sistema, a experiência da HP reconhecida pela indústria fornece suporte do tipo missão crítica como base da configuração de Sistemas Críticos.Esta configuração é o nível mínimo de serviço para ambientes de missão crítica. Ela aumenta a prioridade dos serviços reativos e adiciona serviços de suporte proativos com monitoramento da disponibilidade.

sua infra-estrutura sempre ativa potencializa soluções robustas para os principais aplicativos da atualidade

Planejamento de Recursos Corporativos (ERP): A estrutura fundamental para novas áreas de vantagem competitiva: supply chain, e-commerce e desenvolvimento de produtos.
Computação de Missão Crítica: Produtos e soluções de alta disponibilidade para ajudá-lo a obter os níveis de disponibilidade que você precisa para atender a seus clientes.
E-Intelligence: Obtenha o máximo de valor de seus ativos de dados — tanto internos quanto externos — utilizando ferramentas de ponta para análise, business intelligence e aplicativos da HP.
E-commerce: Gerencie os custos de sites de e-commerce, refinando os recursos de computação para atender as necessidades que estão sempre mudando e assegurar que seu site de e-commerce crítico esteja disponível e possua a capacidade que necessita.
Computação Técnica: Os aplicativos de computação técnica nunca conseguem obter poder suficiente. Os níveis extremamente altos de desempenho e capacidade de expansão oferecidos por uma infra-estrutura sempre ativa atendem a essas necessidades de frente.
Consolidação de Sistemas: Reduza os custos, aumente a flexibilidade, a disponibilidade e o desempenho, e melhore o gerenciamento das infra-estruturas de TI com a complexidade reduzida e a disponibilidade ampliada das configurações sempre ativa.

Ela inclui a Configuração Básica, acrescida de:

- Um plano de suporte detalhando os requisitos específicos da conta em questão e o compromisso de resposta do HP
- Engenheiros de Conta Designados
- Análise de Prontidão do Superdome para ajudá-lo a atender a seus requisitos de alta disponibilidade e desempenho
- Tópicos de Consultoria Técnica para seleção
- Diagnóstico remoto de alta velocidade e coleta de dados críticos para acompanhar o desempenho do sistema e prevenir problemas antes que ocorram
- Compromisso de resposta em 6 horas para chamadas de reparo de hardware
- Recuperação de Sistema Prioritário
- Serviços de Recuperação de Negócios (opcional)

configuração de continuidade de negócios

A Configuração de Continuidade de Negócios fornece muito mais do que uma lista de serviços. Ela fornece uma forma diferente de abordagem para o planejamento da disponibilidade. A Continuidade de Negócios é uma colaboração entre a HP e o cliente, criando um plano para abordar de forma pró-ativa todos os elementos do ambiente de TI que afetam a disponibilidade dos negócios. Ela foi projetada e construída tendo como meta a disponibilidade máxima e seu foco é na operação ideal dos negócios. A Continuidade de Negócios fornece serviços proativos sofisticados e o melhor serviço de suporte da indústria.

Ela inclui a Configuração Básica e a de Sistemas Críticos, além de:

- Uma equipe dedicada à conta e um plano personalizado de serviços proativos
- Resposta de prioridade máxima fornecida por especialistas treinados
- Processos de gerenciamento de mudanças altamente detalhados
- Revisões de conta mensais
- O único compromisso de resposta em 4 horas para chamadas de restauração de hardware e software da indústria
- Solução permanente de software dentro de 14 dias

novos sistemas operacionais para a era da internet

O ambiente operacional HP-UX 11i fornece a melhor plataforma para empresas de Internet do tipo sempre ativa.

- **O sistema operacional Microsoft® Windows NT®/Linux mais amigável atualmente**, com um ambiente de desenvolvimento Linux Open Source e suporte a WebGain Studio.
- **A melhor funcionalidade ponta-a-ponta de Internet crítica**, alta disponibilidade de sistema único, capacidade de gerenciamento, segurança e integração UNIX/Windows®
- **Desempenho e capacidade de expansão definitivos** com capacidade sob demanda instantânea, suporte a particionamento físico e virtual, forte desempenho Java™ e capacidade de exponsão para Symmetric Multi-Processing (SMP) de 64 processadores de alto desempenho
- **A melhor proteção e longevidade de investimentos** através de compatibilidade binária com os processadores PA-RISC (64 bits) e Itanium Processor Family (IPF)
- **Três opções de conjuntos de capacidade de gerenciamento HP-UX Service Control** para um controle centralizado e capacidade otimizada eficazes quanto ao custo
- **Três opções de ambientes operacionais completos** feitos sob medida para as necessidades de computação de Internet, corporativas ou de missão crítica

ECT 5037 Folha CPL - AC

visão rápida do hp superdome

recursos	benefícios
disponibilidade	
Adição e substituição on-line de placas de E/S PCI, comportimentos de placas de E/S e células (CPU/memória*) 6 ou 12 ventiladores e 4, 6 ou 12 fontes de alimentação, todos hot swap, incluindo N+1 Verificação e correção de erros em todos os caminhos de CPU e memória Caminhos de dados de E/S com proteção de paridade Fonte de alimentação dupla	Recursos de alta disponibilidade embutidos fornecem níveis superiores de • confiabilidade • capacidade de suporte • capacidade de reparos • disponibilidade de sistema único • disponibilidade de sistemas múltiplos para ajudar a obter o máximo de tempo ativa para aplicativos de missão crítica
até 16 partições físicas (nPartitions)	Fornece capacidade de particionamento físico
HP Virtual Partitions (vPar) até 64	Fornece capacidade de particionamento lógico
Suporte a soluções de cluster local e remoto para projetos de site backup com distância ilimitada	Soluções completas para alta disponibilidade em clusters eliminam os pontos de falha individuais
capacidade	
Nó único: 1 a 64 de 552MHz, 750MHz, 875MHz	Permite expansão de diferentes processadores no mesmo gabinete. A estrutura do servidor superdome também aceitará novos processadores PA-RISC
CPUs de alto desempenho P A-8700+ com 2.25MB de cache on-chip por CPU	
Desempenho de liderança	Seus benchmarks são recordes mundiais e um padrão para a indústria
Capacidade de particionamento (1 a 16 nPartitions) para alocação de recursos, diversos ambientes operacionais ou escalonamento de aplicativos Até 64 partições virtuais	Permite que o gerenciador do sistema otimize a alocação de recursos entre cargas de trabalho concorrentes. Quando utilizondo 16 nPartitions não existe perdas de escalabilidade, pois com 64 CPUs o servidor mantém suas capacidades máximos de memório e slots PCI para proteger os investimentos em hardware
Até 256 GB de memória (512GB previsto para julho 2003) Largura de banda de memória de 64GB/s por gabinete de 64 CPU	Desempenho de subsistema de memória aumentado para o processamento rápido e confiável de aplicativos de alto desempenho
P[illegible]drão da indústria de 64 bits 33MHz (2x) ou 66MHz (4x) [illegible], canais de E/S de 265MB/s (PCI de 33MHz) ou 530MB/s (PCI de 66MHz) Até 192 slots PCI hot swap de E/S (com gabinete para expansão de E/S)	Manipula facilmente aplicativos com muitas operações de I/O e possibilita um escalanamento rápido para acomodar demandas mais altas
Opções de armazenamento incluindo arrays de disco JBOD, Fibre Channel ou HP Surestore; HP AutoRAID, Multiplexador HP Fibre-Channel-to-SCSI, unidades de fita e bibliotecas	Armazenamento flexível de alta capacidade que protege os dadas críticos
conectividade	
Operações básicas de E/S incluindo LAN 10/100Base-T	Capacidade de conexão em rede fácil e pronta para funcionar
Conectividade de rede: para Token Ring, 1000Base-SX, 1000Base-T, 10/100Base-TX, Terminal MUX, PKC, HIPPI, X.25, ATM, Hyperfabric e FDDI	Soluções completas de conectividade ponta-a-ponta para e-services
Conectividade de armazenamento: Ultra2 SCSI, F/W SCSI, Fibre Channel	Grande variedade de opções de conectividade de armazenamento de alta velocidade
Suporte a servidor WAP Nokia	Conectividade para aplicativos sem fio
segurança	
Detecção de invasão baseada no host	Segurança e proteção definitivas contra ataques
Capacidade de rede virtual privada IPSec ponta-a-ponta	Segurança de camada de rede independente de aplicativo
capacidade de gerenciamento	
Estação de Gerenciamento de Suporte	Acesso remoto centralizado a firmware e ferramentas de diagnóstico de varredura, para uso em todos os sistemas Superdome no centro de processamento de dados
Gerenciador de Partições (parmgr)	Interface GUI intuitiva para gerenciar e modificar facilmente todos as partições de um sistema Superdome
Sistema de Gerenciamento de Falhas Estendido	Console para a exibição do status do sistema (local e remoto), restauração do sistema, poder de controle para ligar e desligar
HP WebQoS Peak integrado	Estabiliza o desempenho de sites na Web sob cargas muito pesadas para melhorar a confiabilidade do site e a produção de transações
H[illegible]rvicecontrol Manager integrado	Controle central dos recursos do servidor rápida e eficoz quanto oos custos para o mais alto grau de eficiência na administração do sistema
HP-UX Workload Manager	Primeiro gerenciamento de recursos baseado em metas da indústria UNIX. Reconfigura automaticamente as alocações de CPU, baseado nos objetivos de nível de serviço do cliente (SLOs)
proteção e flexibilidade dos investimentos	
Projetado para atualizações futuras para diversas gerações de PA-RISC e IPF	Proteção superior dos investimentos e longevidade
Licença ilimitado embutida para o sistema operacional de Internet HP-UX 11i; opções de atualização para o Enterprise ou Mission-Critical HP-UX	Opção de escolha entre três ambientes operacionois com todos os componentes básicos de sistema operacional necessários para ombientes de Internet, corporativos ou de missão crítica
Suporte futuro a Windows NT e Linux	Oferece uma seleção de ambientes com transição fócil para a produção na robusta plataforma HP-UX 11i
Seleção de opções integrados de servidor Web: padrão da indústria para um desempenho mais rápido e mais expansível	Focilidade de distribuição para novos sites na Web ou otimizado para sites com alto tráfego
Plataforma de software aberto E-speak para o desenvolvimento e distribuição de e-services	Possibilito a descoberta dinâmica e interação de aplicativos e e-services através da Internet, incluindo capacidades de agenciamento

*Disponível em versões futuras do HP-UX

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1437
Fls: 3
Doc: 3701

ajudando a construir uma infra-estrutura sempre ativa para seu centro de processamento de dados da internet

opções de configuração	hp superdome
Arquitetura SMP (Symetric Multi Processing)	1 a 64 CPU de alto desempenho
placas de células de 4 CPUs[1]	1-16
memória mínima/máxima (com DIMMs de 512 MB), com proteção ECC	2GB/256GB
compartimentos para placa de E/S de 12 slots completamente hot-swap	até 16
slots de E/S PCI completamente hot-swap	até 192 com gabinete de expansão para E/S) (128 slots de 33MHz, 64 slots de 66MHz)
fontes de alimentação redundantes hot-swap (N+1 incluído)	12
ventiladores de E/S	12
ventiladores redundantes hot-swap (N+1 incluído)	8
particionamento físico (nPartitions)	até 16
largura de banda transversal	64GB/s
controladora de célula para largura de banda de subsistema de E/S	2.0GB/s
largura de banda de E/S	32GB/s
largura de banda de memória	64GB/s
sistema operacional	HP-UX 11i
dimensões físicas: altura largura profundidade peso	 1,96 m 1.524 mm 1.220 mm 1.196 kg
temperatura de operação	15°C a 35°C
Tensão nominal de alimentação e freqüência	200 a 240 volts - 50Hz ou 60Hz
taxa máxima de variação de temperatura	20°C/h
umidade relativa de operação	15% a 80%, a 35°C
umidade relativa fora de operação	90% a 650
altitude de operação	0 a 3000m
altitude fora de operação	0 a 4500m

[1]Capacidade de substituição e adição online oferecida com a HP-UX versão posterior a 11i

para mais informações
Visite nosso site sobre os servidores HP Superdome na Web em:
http://www.hp.com/go/superdome

faça seu pedido on-line agora
As informações sobre produtos e documentação técnica da HP estão disponíveis on-line em **www.docs.hp.com**

invent

Itanium é marca comercial da Intel Corporation nos Estados Unidos e em outros países e é usada sob licença. Java é marca comercial da Sun Microsystems, Inc nos Estados Unidos. Microsoft, Windows e Windows NT são marcas registradas da Microsoft Corp nos Estados Unidos. UNIX é marca registrada do The Open Group. Todos os nomes de produtos são marcas comerciais de seus respectivos proprietários. As informações contidas neste documento estão sujeitas a alterações sem aviso prévio. © Copyright Hewlett-Packard Company 2001.
5980-7359PTL

Apêndice DP

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1438
Doc: 3701

E T
4887
Paula
1
AC

Extent-Based Allocation

Disk space is allocated in 1024-byte sectors to form logical blocks. VxFS supports logical block sizes of 1024, 2048, 4096, and 8192 bytes. The default block size is 1K for file systems up to 8 GB, 2K for file systems up to 16 GB, 4K for file systems up to 32 GB, and 8K for file systems beyond this size.

An *extent* is defined as one or more adjacent blocks of data within the file system. An extent is presented as an *address-length* pair, which identifies the starting block address and the length of the extent (in file system or logical blocks). VxFS allocates storage in groups of extents rather than a block at a time (as seen in the HFS file system).

Extents allow disk I/O to take place in units of multiple blocks if storage is allocated in consecutive blocks. For sequential I/O, multiple block operations are considerably faster than block-at-a-time operations; almost all disk drives accept I/O operations of multiple blocks.

The Extent allocation only slightly alters the interpretation of addressed blocks from the inode structure compared to block based inodes. HFS file system inode structure contains the addresses of 12 direct blocks, one indirect block, and one double indirect block. An indirect block contains the addresses of other blocks. The HFS indirect block size is 8K and each address is 4 bytes long. HFS inodes therefore can address 12 blocks directly and up to 2048 more blocks through one indirect address.

A VxFS inode is similar to the HFS inode and references 10 direct extents, each of which are pairs of starting block addresses and lengths in blocks. The VxFS inode also points to two indirect address extents, which contain the addresses of other extents:

- The first indirect address extent is used for single indirection; each entry in the extent indicates the starting block number of an indirect data extent.
- The second indirect address extent is used for double indirection; each entry in the extent indicates the starting block number of a single indirect address extent.

Each indirect address extent is 8K long and contains 2048 entries. All indirect data extents for a file must be the same size; this size is set when the first indirect data extent is allocated and stored in the inode. Directory inodes always use an 8K indirect data extent size. Regular file

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1439
Fls: 3701
Doc:

inodes also use an 8K default indirect data extent size but allocate the indirect data extents in clusters to simulate larger extents.

Typed Extents

NOTE The information in this section applies to the VxFS Version 3 and 4 disk layout.

In Version 3 and 4, VxFS introduced a new inode block map organization for indirect extents known as *typed extents*. Each entry in the block map has a typed descriptor record containing a type, offset, starting block, and number of blocks.

Indirect and data extents use this format to identify logical file offsets and physical disk locations of any given extent. The extent descriptor fields are defined as follows:

type	Uniquely identifies an extent descriptor record and defines the record's length and format.
offset	Represents the logical file offset in blocks for a given descriptor. Used to optimize lookups and eliminate hole descriptor entries.
starting block	The starting file system block of the extent.
number of blocks	The number of contiguous blocks in the extent.

- Indirect address blocks are fully typed and may have variable lengths up to a maximum and optimum size of 8K. On a fragmented file system, indirect extents may be smaller than 8K depending on space availability. VxFS always tries to obtain 8K indirect extents but resorts to smaller indirects if necessary.
- Indirect Data extents are variable in size to allow files to allocate large, contiguous extents and take full advantage of VxFS's optimized I/O.
- Holes in sparse files require no storage and are eliminated by typed records. A hole is determined by adding the offset and length of a descriptor and comparing the result with the offset of the next record.
- While there are no limits on the levels of indirection, lower levels are expected in this format since data extents have variable lengths.
- This format uses a type indicator that determines its record format and content and accommodates new requirements and functionality

E. C. T. 4885 Paula AC

for future types.

The current typed format is used on regular files only when indirection is needed. Typed records are longer than the previous format and require less direct entries in the inode. Newly created files start out using the old format which allows for ten direct extents in the inode. The inode's block map is converted to the typed format when indirection is needed to offer the advantages of both formats.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1440
Fls:
3791
Doc:

Extent Attributes

VxFS allocates disk space to files in groups of one or more extents. HP OnLineJFS also allows applications to control some aspects of the extent allocation. *Extent attributes* are the extent allocation policies associated with a file.

The `setext` and `getext` commands allow the administrator to set or view extent attributes associated with a file, as well as to preallocate space for a file. Refer to Chapter 3 , "Extent Attributes," Chapter 6 , "Application Interface," `setext`(1M), and `getext`(1M) for discussions on how to use extent attributes.

The `vxtunefs` command allows the administrator to set or view the default indirect data extent size. Refer to Chapter 5 , "Performance and Tuning" and `vxtunefs`(1M) for discussions on how to use the indirect data extent size feature.

NOTE `setext` functionality is available only with the optional HP OnLineJFS product.

Fast File System Recovery

The HFS file system relies on full structural verification by the `fsck` utility as the only means to recover from a system failure. For large disk configurations, this utility involves a time consuming process of checking the entire structure, verifying that the file system is intact, and correcting any inconsistencies.

VxFS provides recovery only seconds after a system failure by utilizing a tracking feature called *`intent logging`*. This feature records pending changes to the file system structure in a circular *`intent log`*. During system failure recovery, the VxFS `fsck` utility performs an intent log replay, which scans the intent log and nullifies or completes file system operations that were active when the system failed. The file system can then be mounted without completing a full structural check of the entire file system. The intent log recovery feature is not readily apparent to the user or the system administrator except during a system failure.

Replaying the intent log may not completely recover the damaged file system structure if the disk suffers a hardware failure; such situations may require a complete system check using the `fsck` utility provided with VxFS.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1441
Doc: 3701

Online System Administration

With the HP OnLineJFS product, a VxFS file system can be defragmented and resized while it remains online and accessible to users. The following sections contain detailed information about these features.

NOTE The online administration features, defragmentation, resizing, and online backup, are available only with the optional HP OnLineJFS product.

Defragmentation

Free resources are initially aligned and allocated to files in the most efficient order possible to provide optimal performance. On an active file system, the original order of free resources is lost over time as files are created, removed, and resized. The file system is spread further and further along the disk, leaving unused gaps or *fragments* between areas that are in use. This process is also known as *fragmentation* and leads to degraded performance because the file system has fewer options when assigning a file to an extent (a group of contiguous data blocks).

The HFS file system uses the concept of *cylinder groups* to limit fragmentation. Cylinder groups are self-contained sections of a file system that indicate free inodes and data blocks. Allocation strategies in HFS attempt to place inodes and data blocks in close proximity. This reduces fragmentation but does not eliminate it.

HP OnLineJFS provides the online administration utility `fsadm` to resolve the problem of fragmentation. The `fsadm` utility defragments a mounted file system by:

- removing unused space from directories
- making all small files contiguous
- consolidating free blocks for file system use

This utility can run on demand and should be scheduled regularly as a `cron` job.

E C T
4881
Paulo

Resizing

A file system is assigned a specific size as soon as it is created; the file system may become too small or too large as changes in file system usage take place over time.

The HFS file system traditionally offers four solutions to address an inadequate small file system:

- Move some users to a different file system.
- Move a subdirectory of the file system to a new file system.
- Copy the entire file system to a larger file system.
- Unmount the file system (offline), extend the volume, extend the file system, then remount the file system.

Most large file systems with too much space try to reclaim the unused space by off-loading the contents of the file system and rebuilding it to a preferable size. The HFS file system requires unmounting the file system and blocking user access during the modification.

When the HP OnLineJFS product is installed, the VxFS utility `fsadm` can expand or shrink a file system without unmounting the file system or interrupting user productivity. However, to expand a file system, the underlying device on which it is mounted must be expandable. LVM facilitates expansion using virtual disks that can be increased in size while in use. The VxFS and LVM packages complement each other to provide online expansion capability.

NOTE

You can only shrink a file system that uses the version 4 disk layout. However, even with the version 4 disk layout, it is sometimes not possible to shrink a file system. When shrinking a version 4 file system, JFS attempts to move extents off the area of the file system being reduced. However, if JFS cannot move extents off the area of the file system being reduced, the shrink will fail.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1442
Fls:
Doc: 3701

Online Backup

The HP OnLineJFS product provides a method of online backup of data using the *snapshot* feature. An image of a mounted file system instantly becomes an exact read-only copy of the file system at a certain point in time. The original file system is *snapped* while the copy is called the *snapshot*.

When changes are made to the snapped file system, the old data is first copied to the snapshot. When the snapshot is read, data that has not changed is read from the snapped file system. Changed data is read directly from the snapshot.

Backups require one of the following methods:

- copying selected files from the snapshot file system (using `find` and `cpio`)
- backing up the entire file system (using `fscat`)
- initiating a full or incremental backup (using `vxdump`)

For detailed information about performing online backups, see Chapter 4 , "Online Backup."

E C T
4879 Paulo
A C

Application Interface

The VxFS file system conforms to the System V Interface Definition (SVID) requirements and supports user access through the Network File System (NFS). Applications that require performance features not available with other file systems can take advantage of VxFS enhancements that are introduced in this section and covered in detail in Chapter 6 , "Application Interface."

Application Transparency

In most cases, any application designed to run on the HFS file system should run transparently on the VxFS file system.

Expanded Application Facilities

The HP OnLineJFS product provides some facilities frequently associated with commercial applications that make it possible to:

- preallocate space for a file
- specify a fixed extent size for a file
- bypass the system buffer cache for file I/O
- specify the expected access pattern for a file

Since these facilities are provided using VxFS-specific ioctl system calls, most existing UNIX system applications do not use these facilities. The `cp`, `cpio`, and `mv` utilities use these facilities to preserve extent attributes and allocate space more efficiently. The current attributes of a file can be listed using the `getext` command or `ls` command. The facilities can also improve performance for custom applications. For portability reasons, these applications should check what file system type they are using before using these interfaces.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1443
Doc: 3701

Extended mount Options

The VxFS file system supports extended `mount` options to specify:

- enhanced data integrity modes
- enhanced performance modes
- temporary file system modes
- improved synchronous writes

See Chapter 5 , "Performance and Tuning" and `mount_vxfs`(1M) for details on the VxFS `mount` options.

Enhanced Data Integrity Modes

NOTE Performance trade-offs are associated with these `mount` options.

The HFS file system is "buffered" in the sense that resources are allocated to files and data is written asynchronously to files. In general, the buffering schemes provide better performance without compromising data integrity.

If a system failure occurs during space allocation for a file, uninitialized data or data from another file may appear in the extended file after reboot. Data written shortly before the system failure may also be lost.

Using blkclear for Data Integrity

In environments where performance is more important than absolute data integrity, the preceding situation is not of great concern. However, VxFS supports environments that emphasize data integrity by providing the `mount -o blkclear` option that ensures uninitialized data does not appear in a file.

Using closesync for Data Integrity

VxFS provides the `mount -o mincache=closesync` option, which is useful in desktop environments with users who are likely to shut off the power on machines without halting them first. In `closesync` mode, only

files that are written during the system crash or shutdown can lose data. Any changes to a file are flushed to disk when the file is closed.

Enhanced Performance Mode

The HFS file system is asynchronous in the sense that structural changes to the file system are not immediately written to disk. File systems are designed this way to provide better performance. However, recent changes to the file system may be lost if a system failure occurs. More specifically, attribute changes to files and recently created files may disappear.

The default logging mode provided by VxFS (`mount -o log`) guarantees that all structural changes to the file system are logged to disk before the system call returns to the application. If a system failure occurs, `fsck` replays any recent changes to preserve all metadata. Recent file data may be lost unless a request was made to `sync` it to disk.

Using delaylog for Enhanced Performance

VxFS provides the `mount -o delaylog` option which increases performance by delaying the logging of some structural changes. However, recent changes may be lost during a system failure. This option provides at least the same level of data accuracy that traditional UNIX file systems provide for system failures, along with fast file system recovery.

Temporary File System Modes

On most UNIX systems, temporary file system directories (such as `/tmp` and `/usr/tmp`) often hold files that do not need to be retained when the system reboots. The underlying file system does not need to maintain a high degree of structural integrity for these temporary directories.

Using tmplog for Temporary File Systems

VxFS provides a `mount -o tmplog` option which allows the user to achieve higher performance on temporary file systems by delaying the logging of most operations.

Improved Synchronous Writes

HP OnLineJFS provides superior performance for synchronous write

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1444
Fls:
Doc: 3701

applications.

The default `datainlog` option to `mount` greatly improves the performance of small synchronous writes.

The `convosync=dsync` option to `mount` improves the performance of applications that require synchronous data writes but not synchronous inode time updates.

NOTE The use of the `convosync=dsync` option violates POSIX semantics.

NOTE The `datainlog` and `convosync` options are available only with the optional HP OnLineJFS product.

E C T
4875
Paula
AC

Enhanced I/O Performance

VxFS provides enhanced I/O performance by applying an aggressive I/O clustering policy.

Enhanced I/O Clustering

I/O clustering is a technique of grouping multiple I/O operations together for improved performance. The VxFS I/O policies provide more aggressive clustering processes than other file systems and offer higher I/O throughput when using large files; the resulting performance is comparable to that provided by raw disk.

Application-Specific Parameters

System administrators can also set application specific parameters on a per-file system basis to improve I/O performance.

- Default Indirect Extent Size

  On disk layout Version 2, this value can be set up to apply to all the indirect extents, provided a fixed extent size is not already set and the file does not already have indirect extents. The Version 3 and 4 disk layout uses typed extents which have variable sized indirects.

- Discovered Direct I/O

  All sizes above this value would be performed as direct I/O.

NOTE The Discovered Direct I/O parameter is available only with the HP OnLineJFS product.

- Maximum Direct I/O Size

  This value defines the maximum size of a single direct I/O.

NOTE The Maximum Direct I/O Size parameter is available only with the HP OnLineJFS product.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1445
Fls:
Doc: 3701
3701

For a discussion of performance benefits, refer to Chapter 5 , "Performance and Tuning", Chapter 6 , "Application Interface", `vxtunefs`(1M), and `tunefstab`(4).

E C T
1873
Paulo
L - AC

Quotas

VxFS supports the Berkeley Software Distribution (BSD) style user quotas, which allocate per-user quotas and limit the use of two principal resources: files and data blocks. The system administrator can assign quotas for each of these resources. Each quota consists of two limits for each resource:

- The *hard limit* represents an absolute limit on data blocks or files. The user may never exceed the hard limit under any circumstances.
- The *soft limit* is lower than the hard limit and may be exceeded for a limited amount of time. This allows users to temporarily exceed limits as long as they fall under those limits before the allotted time expires.

The system administrator is responsible for assigning hard and soft limits to users. See "Quota Limits" for more information.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1446
Fls:
3701
Doc:

Access Control Lists

An Access Control List (ACL) stores a series of entries that identify specific users or groups and their access privileges for a directory or file. A file may have its own ACL or may share an ACL with other files. ACLs have the advantage of specifying detailed access permissions for multiple users and groups. Refer to getacl (1M) and `setacl`(1M) for information on viewing and setting ACLs.

NOTE Access control lists require a file system with the version 4 disk layout.

Support for Large Files

VxFS can, theoretically, support files up to two terabytes in size because file system structures are no longer in fixed locations (see Chapter 2 , "Disk Layout"). The maximum size tested and supported on HP-UX 11.x systems is one terabyte. Large files are files larger than two gigabytes in size.

NOTE Be careful when enabling large file capability. Applications and utilities such as backup may experience problems if they are not aware of large files.

Creating a File System with Large Files

You can create a file system with large file capability by entering the following command:

```
# mkfs -F vxfs -o largefiles special_device size
```

Specifying `largefiles` sets the `largefiles` flag, which allows the file system to hold files up to one terabyte in size. Conversely, the default `nolargefiles` option clears the flag and limits files being created to a size of two gigabytes or less:

```
# mkfs -F vxfs -o nolargefiles special_device size
```

NOTE The `largefiles` flag is persistent and stored on disk.

Mounting a File System with Large Files

If a mount succeeds and `nolargefiles` is specified, the file system cannot contain or create any large files. If a mount succeeds and `largefiles` is specified, the file system may contain and create large files.

The `mount` command fails if the specified `largefiles|nolargefiles` option does not match the on-disk flag.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1447
Fls:
3701
Doc:

The `mount` command defaults to match the current setting of the on-disk flag if specified without the `largefiles` or `nolargefiles` option, so it's best not to specify either option. After a file system is mounted, you can use the `fsadm` utility to change mount options.

Managing a File System with Large Files

You can determine the current status of the largefiles flag with any of the following commands:

```
# mount
# mkfs -F vxfs -m  special_device
# fsadm -F vxfs  mount_point
```

You can switch capabilities on a mounted file system with the `fsadm` command:

```
# fsadm -F vxfs -o largefiles|nolargefiles mount_point
```

You cannot switch a file system to `nolargefiles` if it holds large files.

See `mount_vxfs`(1M), `fsadm_vxfs`(1M), and `mkfs_vxfs`(1M).

E C T
4869
Disk Layout
L - A

2 Disk Layout

RQS Nº 03/2005 - CN
CPMI - CORREIOS
41
Fls: 1448
Doc: 3701

Introduction

Three disk layouts are available with the VxFS file system:

Version 2	The Version 2 disk layout was designed to support features such as filesets, dynamic inode allocation, and enhanced security.
Version 3	The Version 3 disk layout encompasses all file system structural information in files, rather than at fixed locations on disk, allowing for greater scalability. Version 3 supports files and file systems up to one terabyte in size.
Version 4	The Version 4 disk layout supports access control lists (ACLs).

NOTE The Version 1 disk layout is not supported on HP-UX.

The following topics are covered in this chapter:

- "Disk Space Allocation"
- "The VxFS Version 1 Disk Layout"
- "Overview"
- "Super-Block"
- "Intent Log"
- "Allocation Unit"
- "The VxFS Version 2 Disk Layout"
  - "Overview"
  - "Basic Layout"
  - "Filesets and Structural Files"
  - "Locating Dynamic Structures"
- "The VxFS Version 3 Disk Layout"
- "The VxFS Version 4 Disk Layout"

When HP-UX 11.1x is installed on a system, new VxFS file systems are created with the Version 4 layout by default. When JFS 3.3 is installed on an HP-UX 11.00 system, new file systems are created with the Version 3 layout by default. Although `mkfs` allows the user to specify

E C T
4867
Disk Layout
Introduction
Paula
A C

other disk layouts, it is generally preferable to use the Version 4 layout for new file systems.

The vxupgrade command can upgrade an existing Version 3 VxFS file system to the Version 4 layout while the file system remains online. vxupgrade can also upgrade a Version 2 file system to the Version 3 layout. See vxupgrade(1M) for details on upgrading VxFS file systems.You cannot downgrade a file system that has been upgraded.

NOTE

You cannot upgrade the root (/) or /usr file systems to Version 4 on an 11.00 system running JFS 3.3. Additionally, we do not advise upgrading the /var or /opt file systems to Version 4 on an 11.00 system. These core file systems are crucial for system recovery. The HP-UX 11.00 kernel and emergency recovery media were built with an older version of JFS that does not recognize the Version 4 disk layout. If these file systems were upgraded to Version 4, your system might have errors booting with the 11.00 kernel as delivered, or booting with the emergency recovery media.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1449
Doc 1

Disk Space Allocation

Disk space is allocated by the system in 1024-byte sectors. An integral number of sectors are grouped together to form a logical block. VxFS supports logical block sizes of 1024, 2048, 4096, and 8192 bytes. The default block size is 1024 bytes for file systems less than 3 gigabytes; 2048 bytes for file systems less than 16 gigabytes; 4096 bytes for file systems less than 32 gigabytes; and 8192 bytes for file systems 32 gigabytes or larger. The block size may be specified as an argument to the `mkfs` utility and may vary between VxFS file systems mounted on the same system. VxFS allocates disk space to files in extents. An extent is a set of contiguous blocks.

The VxFS Version 1 Disk Layout

This section describes the VxFS Version 1 disk layout.

NOTE The Version 1 disk layout is not supported on HP-UX.

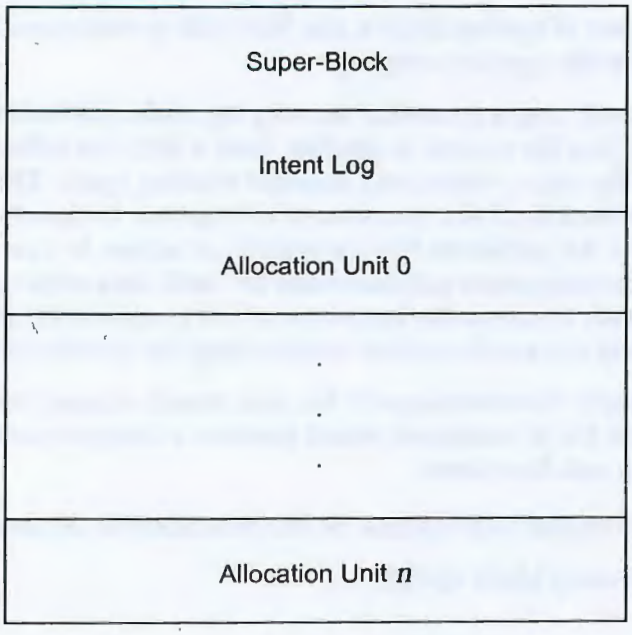
Overview

The VxFS Version 1 disk layout, as shown in Figure 2-1, "VxFS Version 1 Disk Layout" includes:

- the super-block
- the intent log
- one or more allocation units

These elements are discussed in detail in the sections that follow.

Figure 2-1 VxFS Version 1 Disk Layout



RQS Nº 03/2005 - CN
CPMI - CORREIOS
1450
Fls:
3701
Doc:

Super-Block

The super-block contains important information about the file system, such as:

- the file system type
- creation and modification dates
- label information
- information about the size and layout of the file system
- the count of available resources
- the file system disk layout version number

The super-block is always in a fixed location, offset from the start of the file system by 8192 bytes. This fixed location enables utilities to easily locate the super-block when necessary. The super-block is 1024 bytes long.

Copies of the super-block are kept in allocation unit headers: these copies can be used for recovery purposes if the super-block is corrupted or destroyed (see `fsck_vxfs`(1M) for more details).

Intent Log

In the event of system failure, the VxFS file system uses intent logging to guarantee file system integrity.

The *`intent log`* is a circular activity log with a default size of 1024 blocks. If the file system is smaller than 4 MB, the default log size is reduced (by `mkfs_vxfs(1M)`) to avoid wasting space. The intent log contains records of the intention of the system to update a file system structure. An update to the file system structure (a *`transaction`*) is divided into separate sub-functions for each data structure that needs to be updated. A composite log record of the transaction is created, containing the sub-functions constituting the transaction.

For example, the creation of a file that would expand the directory in which the file is contained would produce a transaction consisting of the following sub-functions:

- a free extent map update for the allocation of the new directory block
- a directory block update

E C T
4863
Paulo
I
S

- an inode modification for the directory size change
- an inode modification for the new file
- a free inode map update for the allocation of the new file

VxFS maintains log records in the intent log for all pending changes to the file system structure and ensures that the log records are written to disk in *advance* of the changes to the file system. Once the intent log has been written, the transaction's other updates to the file system can be written in any order. In the event of a system failure, the pending changes to the file system are either nullified or completed by the `fsck` utility. The VxFS intent log generally only records changes to the file system structure. File data changes are not normally logged.

Allocation Unit

An allocation unit is a group of consecutive blocks in a file system that contain a resource summary, free resource maps, inodes, data blocks, and a copy of the super-block. An allocation unit in the VxFS file system is similar in concept to the HFS "cylinder group." Each component of an allocation unit begins on a block boundary. The VxFS Version 1 allocation unit is shown in Figure 2-2, "Allocation Unit Structure."

ROS Nº 03/2005 - CN
CPMI - CORREIOS
1451
Fls:
3701
Doc:

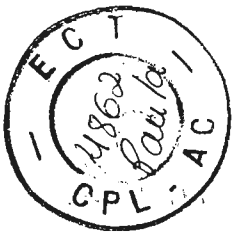
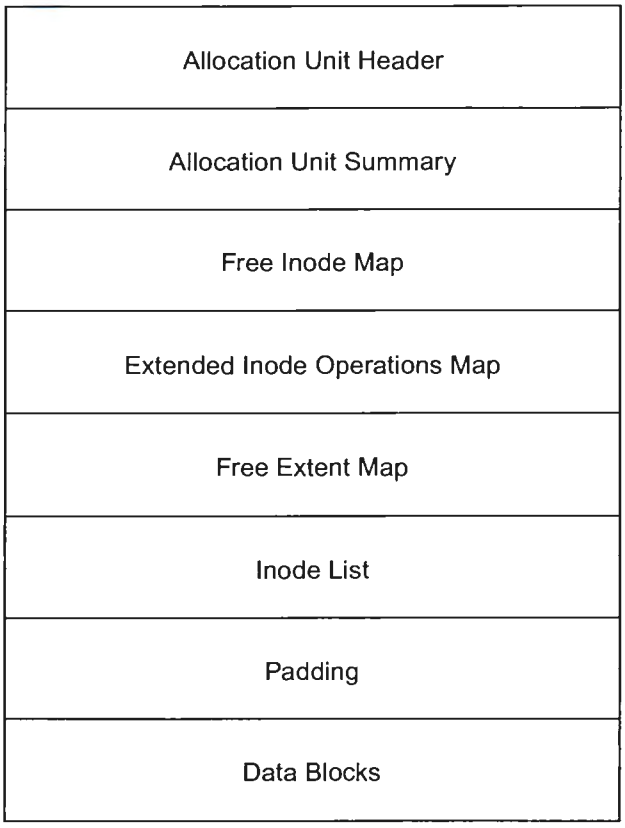


Figure 2-2 **Allocation Unit Structure**



One or more allocation units exist per file system. Allocation units are located immediately after the intent log. The number and size of allocation units can be specified when the file system is made. All of the allocation units, except possibly the last one, are of equal size. If space is limited, the last allocation unit can have a partial set of data blocks to allow use of all remaining blocks.

Allocation Unit Header

The allocation unit header contains a copy of the file system's super-block that is used to verify that the allocation unit matches the super-block of the file system. The super-block copies contained in allocation unit headers can also be used for recovery purposes if the super-block is corrupted or destroyed. The allocation unit header occupies the first block of each allocation unit.

Allocation Unit Summary

The allocation unit summary contains the number of inodes with extended operations pending, the number of free inodes, and the number of free extents in the allocation unit.

Free Inode Map The free inode map is a bitmap that indicates which inodes are free and which are allocated. A free inode is indicated by the bit being on. Inodes zero and one are reserved by the file system; inode two is the inode for the root directory; inode three is the inode for the `lost+found` directory.

Extended Inode Operations Map The extended inode operations map keeps track of inodes on which operations would remain pending for too long to reside in the intent log. The extended inode operations map is in the same format as the free inode map. To prevent the intent log from wrapping and the transaction from getting overwritten, the required operations are stored in the affected inode (if the transaction has not completed, it does not get overwritten, the new log waits and the file system is frozen). This map is then updated to identify the inodes that have extended operations that need to be completed.

Free Extent Map The free extent map is a series of independent 512-byte bitmaps that are each referred to as a free extent map section. Each section is broken down into multiple regions. The first region, of 2048 bits, represents a section of 2048 one-block extents. The second region, of 1024 bits, represents a section of 1024 two-block extents. This regioning continues for all powers of 2 up to the single bit that represents one 2048 block extent.

The file system uses this bitmapping scheme to find an available extent closest in size to the space required. This keeps files as contiguous as possible for faster performance.

Inode List An inode is a data structure that contains information about a file. The VxFS inode size is 256 bytes. Each inode stores information about a particular file such as:

- file length
- link count
- owner and group IDs
- access privileges

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1452
Fls: 3701
Doc:

- time of last access
- time of last modification
- pointers to the extents that contain the file's data

There are up to ten direct extent address size pairs per inode. Each direct extent address indicates the starting block number of a direct extent; direct extent sizes can vary. If all of the direct extents are used, two indirect address extents are available for use in each inode:

- The first indirect address extent is used for single indirection, where each entry in the extent indicates the starting block number of an indirect data extent.
- The second indirect address extent is used for double indirection, where each entry in the extent indicates the starting block number of a single indirect address extent.

Each indirect address extent is 8K long and contains 2048 entries. All indirect data extents for a given file have the same size, which is determined when the file's first indirect data extent is allocated.

The inode list is a series of inodes. There is one inode in the list for every file in the file system.

Padding It may be desirable to align data blocks to a physical boundary. To facilitate this, the system administrator may specify that a gap be left between the end of the inode list and the first data block.

Data Blocks The balance of the allocation unit is occupied by data blocks. Data blocks contain the actual data stored in files and directories.

E C T
4863
Paulo
Disk Layout

- an inode modification for the directory size change
- an inode modification for the new file
- a free inode map update for the allocation of the new file

VxFS maintains log records in the intent log for all pending changes to the file system structure and ensures that the log records are written to disk in *advance* of the changes to the file system. Once the intent log has been written, the transaction's other updates to the file system can be written in any order. In the event of a system failure, the pending changes to the file system are either nullified or completed by the `fsck` utility. The VxFS intent log generally only records changes to the file system structure. File data changes are not normally logged.

Allocation Unit

An allocation unit is a group of consecutive blocks in a file system that contain a resource summary, free resource maps, inodes, data blocks, and a copy of the super-block. An allocation unit in the VxFS file system is similar in concept to the HFS "cylinder group." Each component of an allocation unit begins on a block boundary. The VxFS Version 1 allocation unit is shown in Figure 2-2, "Allocation Unit Structure."

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1453
Fls:
Doc: 3701

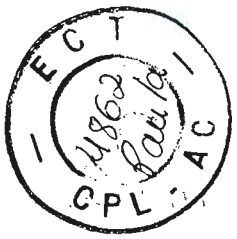
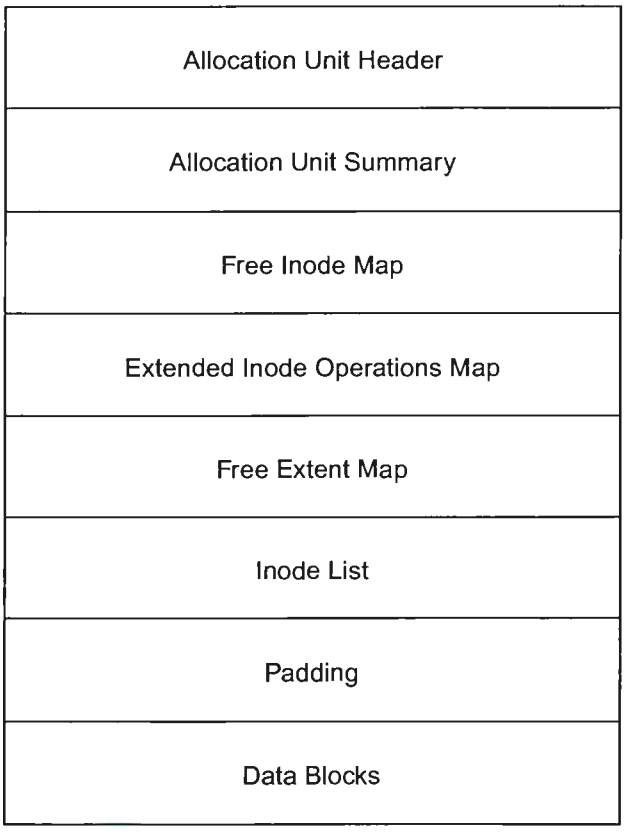


Figure 2-2 **Allocation Unit Structure**



One or more allocation units exist per file system. Allocation units are located immediately after the intent log. The number and size of allocation units can be specified when the file system is made. All of the allocation units, except possibly the last one, are of equal size. If space is limited, the last allocation unit can have a partial set of data blocks to allow use of all remaining blocks.

Allocation Unit Header

The allocation unit header contains a copy of the file system's super-block that is used to verify that the allocation unit matches the super-block of the file system. The super-block copies contained in allocation unit headers can also be used for recovery purposes if the super-block is corrupted or destroyed. The allocation unit header occupies the first block of each allocation unit.

Allocation Unit Summary

The allocation unit summary contains the number of inodes with extended operations pending, the number of free inodes, and the number of free extents in the allocation unit.

Free Inode Map The free inode map is a bitmap that indicates which inodes are free and which are allocated. A free inode is indicated by the bit being on. Inodes zero and one are reserved by the file system; inode two is the inode for the root directory; inode three is the inode for the `lost+found` directory.

Extended Inode Operations Map The extended inode operations map keeps track of inodes on which operations would remain pending for too long to reside in the intent log. The extended inode operations map is in the same format as the free inode map. To prevent the intent log from wrapping and the transaction from getting overwritten, the required operations are stored in the affected inode (if the transaction has not completed, it does not get overwritten, the new log waits and the file system is frozen). This map is then updated to identify the inodes that have extended operations that need to be completed.

Free Extent Map The free extent map is a series of independent 512-byte bitmaps that are each referred to as a free extent map section. Each section is broken down into multiple regions. The first region, of 2048 bits, represents a section of 2048 one-block extents. The second region, of 1024 bits, represents a section of 1024 two-block extents. This regioning continues for all powers of 2 up to the single bit that represents one 2048 block extent.

The file system uses this bitmapping scheme to find an available extent closest in size to the space required. This keeps files as contiguous as possible for faster performance.

Inode List An inode is a data structure that contains information about a file. The VxFS inode size is 256 bytes. Each inode stores information about a particular file such as:

- file length
- link count
- owner and group IDs
- access privileges

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1454
Doc: 3701

- time of last access
- time of last modification
- pointers to the extents that contain the file's data

There are up to ten direct extent address size pairs per inode. Each direct extent address indicates the starting block number of a direct extent; direct extent sizes can vary. If all of the direct extents are used, two indirect address extents are available for use in each inode:

- The first indirect address extent is used for single indirection, where each entry in the extent indicates the starting block number of an indirect data extent.
- The second indirect address extent is used for double indirection, where each entry in the extent indicates the starting block number of a single indirect address extent.

Each indirect address extent is 8K long and contains 2048 entries. All indirect data extents for a given file have the same size, which is determined when the file's first indirect data extent is allocated.

The inode list is a series of inodes. There is one inode in the list for every file in the file system.

Padding It may be desirable to align data blocks to a physical boundary. To facilitate this, the system administrator may specify that a gap be left between the end of the inode list and the first data block.

Data Blocks The balance of the allocation unit is occupied by data blocks. Data blocks contain the actual data stored in files and directories.

The VxFS Version 2 Disk Layout

This section describes the VxFS Version 2 disk layout.

Due to the relatively complex nature of the Version 2 layout, the sections that follow are arranged to cover the following general areas:

- Structural elements of the file system that exist in fixed locations. These elements are discussed in "Basic Layout".
- Structural elements of the file system that do not exist in fixed locations. These elements are discussed in "Filesets and Structural Files".
- The location and use of the various structural elements when the file system is mounted. This is discussed in "Locating Dynamic Structures".

Overview

Many aspects of the Version 1 disk layout are preserved in the Version 2 disk layout. However, the Version 2 layout differs from the Version 1 layout in that it includes support for the following features:

- filesets (sets of files within a file system)
- dynamic inode allocation (allocation of inodes on an as-needed basis)
- enhanced security

The addition of filesets and dynamic allocation of inodes has affected the disk layout in various ways. In particular, many of the file system structures are now located in files (referred to as *structural files*) rather than in fixed disk areas. This provides a simple mechanism for dynamic growth of structures. For example, inodes are now stored in structural files and allocated as needed. In general, file system structures that deal with space allocation are still in fixed disk locations, while most other structures are dynamically allocated and have become clients of the file system's disk space allocation scheme.

The Version 2 disk layout adds BSD-style quota support. The differences include the fileset header structure modification to store a quota inode and preallocation of an internal quotas file.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1455
Fls:
3701
Doc:

Basic Layout

This section describes the structural elements of the file system that exist in fixed locations on the disk.

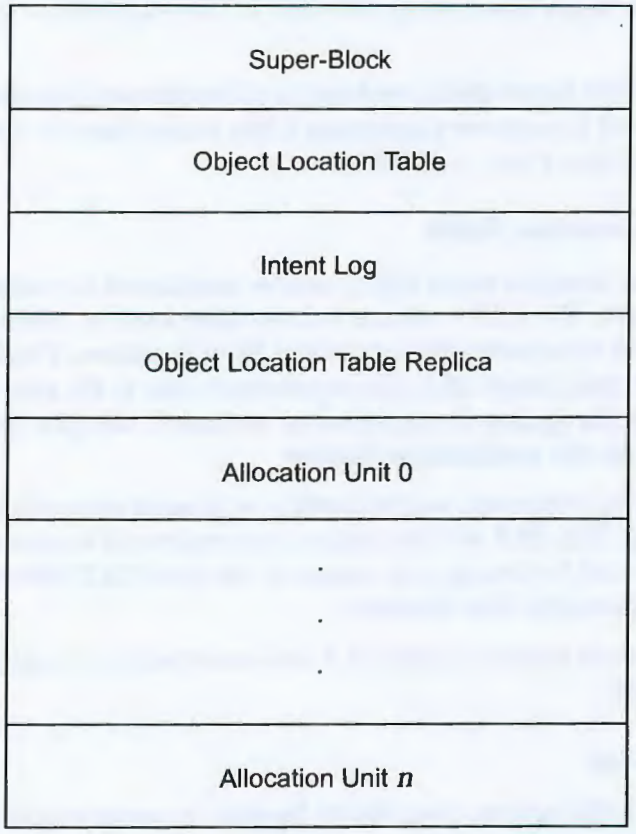
The VxFS Version 2 disk layout is illustrated in Figure 2-3, "VxFS Version 2 Disk Layout" and is composed of:

- the super-block
- the object location table
- the intent log
- a replica of the object location table
- one or more allocation units

These and other elements are discussed in detail in the sections that follow.

E C T
L - AC

Figure 2-3 VxFS Version 2 Disk Layout



Super-Block

The super-block contains important information about the file system, such as

- the file system type
- creation and modification dates
- label information
- information about the size and layout of the file system
- the count of available resources
- the file system disk layout version number
- pointers to the object location table and its replica

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1456
Fls:
Doc: 3701

The super-block is always in a fixed location, offset from the start of the file system by 8192 bytes. This fixed location enables utilities to easily locate the super-block when necessary. The super-block is 1024 bytes long.

Copies of the super-block are kept in allocation unit headers: these copies can be used for recovery purposes if the super-block is corrupted or destroyed (see `fsck_vxfs`(1M)).

Object Location Table

The object location table (OLT) can be considered an extension of the super-block. The OLT contains information used at mount time to locate file system structures that are not in fixed locations. The OLT is typically located immediately after the super-block and is 8K long. However, if a Version 1 file system is upgraded to Version 2, the placement of the OLT depends on the availability of space.

The OLT is replicated and its replica is located immediately after the intent log. The OLT and its replica are separated in order to minimize the potential for losing both copies of the vital OLT information in the event of localized disk damage.

The contents and use of the OLT are described in "Locating Dynamic Structures".

Intent Log

The VxFS file system uses intent logging to guarantee file system integrity in the event of system failure

The *`intent log`* is a circular activity log with a default size of 512 blocks. If the file system is less than 4 MB, the log size will be reduced to avoid wasting space. The intent log contains records of the intention of the system to update a file system structure. An update to the file system structure (a *`transaction`*) is divided into separate sub-functions for each data structure that needs to be updated. A composite log record of the transaction is created that contains the subventions that constitute the transaction.

For example, the creation of a file that would expand the directory in which the file is contained will produce a transaction consisting of the following subventions:

- a free extent map update for the allocation of the new directory block

E C T
21855
Paulo
A C

- a directory block update
- an inode modification for the directory size change
- an inode modification for the new file
- a free inode map update for the allocation of the new file

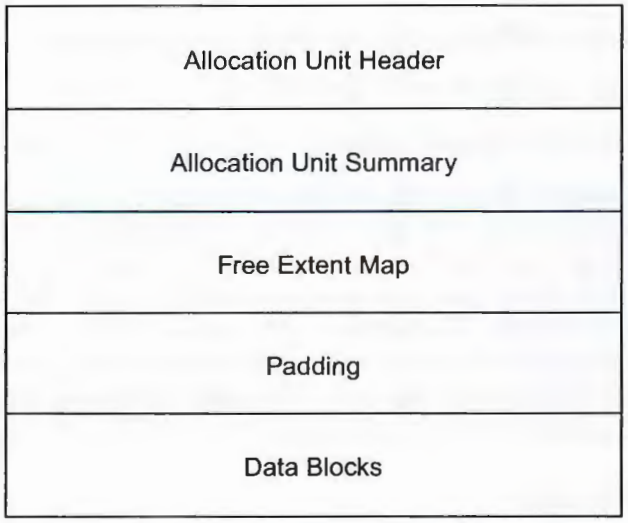
VxFS maintains log records in the intent log for all pending changes to the file system structure, and ensures that the log records are written to disk in *advance* of the changes to the file system. Once the intent log has been written, the transaction's other updates to the file system can be written in any order. In the event of a system failure, the pending changes to the file system are either nullified or completed by the `fsck` utility. The VxFS intent log generally only records changes to the file system structure. File data changes are not normally logged.

Allocation Unit

An allocation unit is a group of consecutive blocks in a file system that contain a resource summary, a free resource map, data blocks, and a copy of the super-block. An allocation unit in the VxFS file system is similar in concept to the HFS "cylinder group." Each component of an allocation unit begins on a block boundary. All of the Version 2 allocation unit components deal with the allocation of disk space. Those components of the Version 1 allocation unit that deal with inode allocation have been relocated elsewhere for Version 2. In particular, the inode list now resides in an inode list file and the inode allocation information now resides in an inode allocation unit (described later). The VxFS Version 2 allocation unit is depicted in Figure 2-4, "Allocation Unit Structure."

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1457
Doc: 3701

Figure 2-4 **Allocation Unit Structure**



One or more allocation units exist per file system. Allocation units are located after the OLT replica. The number and size of allocation units can be specified when the file system is made. All of the allocation units, except possibly the last one, are of equal size. If space is limited, the last allocation unit can have a partial set of data blocks to allow use of all remaining blocks.

Allocation Unit Header The allocation unit header contains a copy of the file system's super-block that is used to verify that the allocation unit matches the super-block of the file system. The super-block copies contained in allocation unit headers can also be used for recovery purposes if the super-block is corrupted or destroyed. The allocation unit header occupies the first block of each allocation unit.

Allocation Unit Summary The allocation unit summary summarizes the resources (data blocks) used in the allocation unit. This includes information such as the number of free extents of each size in the allocation unit.

Free Extent Map The free extent map is a series of independent 512-byte bitmaps that are each referred to as a free extent map section. Each section is broken down into multiple regions. The first region of 2048 bits represents a section of 2048 one-block extents. The second region of 1024 bits represent a section of 1024 two-block extents. This regioning continues for all powers of 2 up to the single bit that represents

one 2048 block extent.

The file system uses this bitmapping scheme to find an available extent closest in size to the space required. This keeps files as contiguous as possible for faster performance.

Padding It may be desirable to align data blocks to a physical boundary. To facilitate this, the system administrator may specify that a gap be left between the end of the free extent map and the first data block. See Chapter 6 , "Application Interface," for additional information on alignment.

Data Blocks The balance of the allocation unit is occupied by data blocks. Data blocks contain the actual data stored in files and directories.

Filesets and Structural Files

This section describes the structural elements of the file system that are not necessarily in fixed locations on the disk.

With the Version 2 layout, many structural elements of the file system are encapsulated in files to allow dynamic allocation of the file system structure. Files that store this file system structural data are referred to as *structural files*. As the file system grows, more space is allocated to the structural files. Structural files are intended for file system use only and are not generally visible to users.

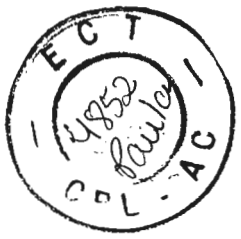
The Version 2 layout supports *filesets*, which are collections of files that exist within a file system. In the current release, each file system contains two filesets:

attribute fileset	A special fileset that stores the structural elements of the file system in the form of structural files. These files are a property of the file system and are not normally visible to the user.
primary fileset	A fileset that contains files that are visible to and accessible by users.

Structural files exist in the attribute fileset only and include thefollowing:

fileset header file	A file that contains a series of fileset headers.
inode list file	A file that contains a series of inodes.

ECT 4853 Fls: 1
ROS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1458
Doc: 3701



inode allocation unit (IAU) file	A file that contains a series of inode allocation units.
current usage table (CUT) file	A file that contains a series of fileset usage entries.
link count table file	A file that contains a link count for each inode in the attribute fileset.
quotas file	A file containing user quota information (for the primary fileset only).

Structural files and their components are discussed in the sections that follow.

Although structural files are contained in the structural fileset, they can "belong" to another fileset. For example, the inode list file for the primary fileset is in the structural fileset, but the structural details that it contains are only applicable to the primary fileset.

Each fileset is defined by structural files as follows:

- an inode list file, which contains the inodes belonging to the fileset
- an inode allocation unit file, which contains a series of inode allocation units
- an entry in the fileset header file, which contains one fileset header per fileset
- an entry in the current usage table file, which contains usage information for each fileset

In addition, the primary fileset has a user quotas file and the structural fileset has a link count table file.

Fileset metadata that cannot be reconstructed using the inode list is replicated to help `fsck` reconstruct the file system in the event of disk damage.

Figure 2-5, "Filesets and Structural Files" shows a fileset and the structural files by which it is defined.

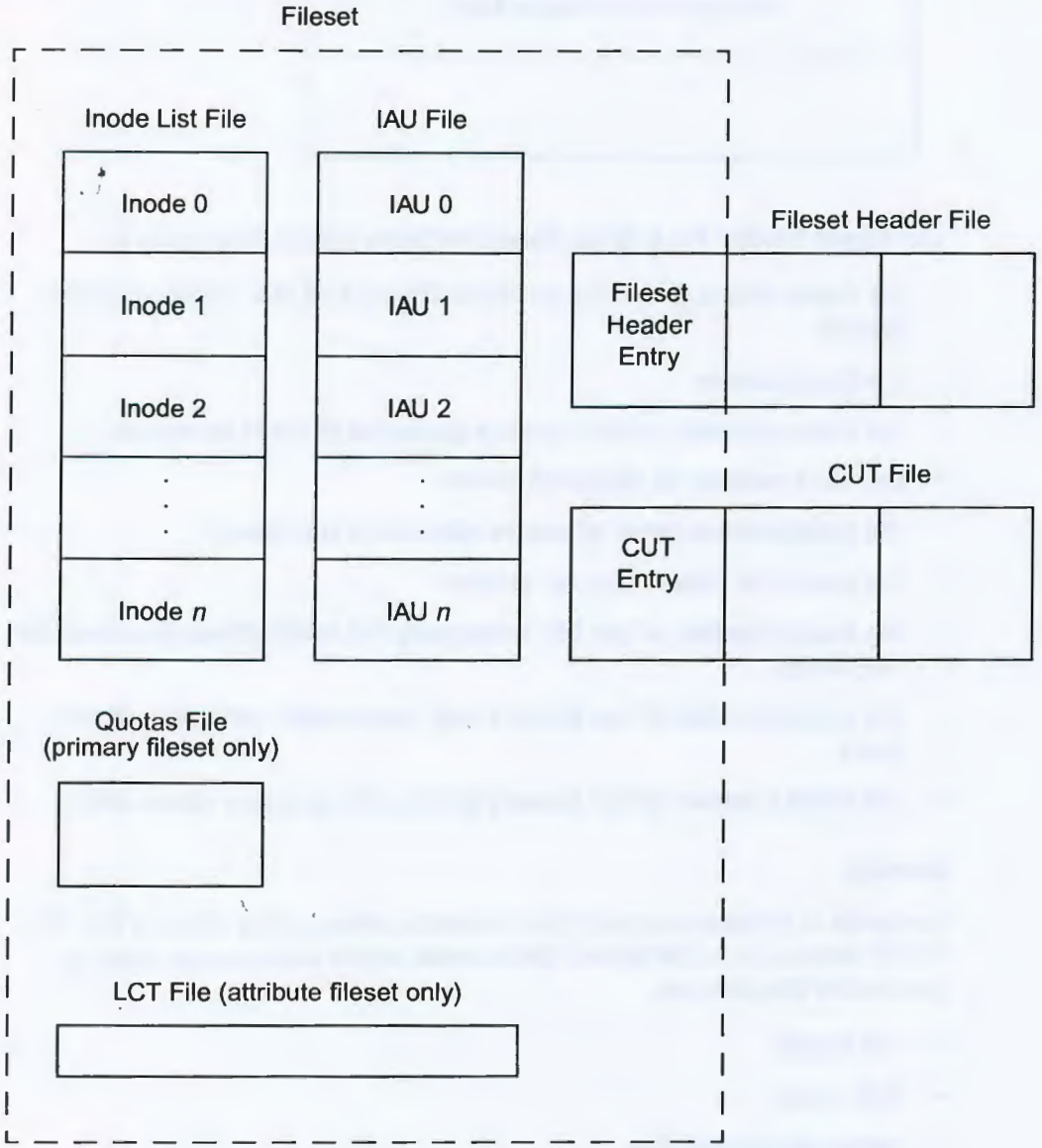
Fileset Header

Each fileset has a header containing information about the fileset's contents and characteristic. All fileset headers are stored in a single fileset header file in the attribute fileset. The fileset header file contains

E C T
485
São Paulo
S

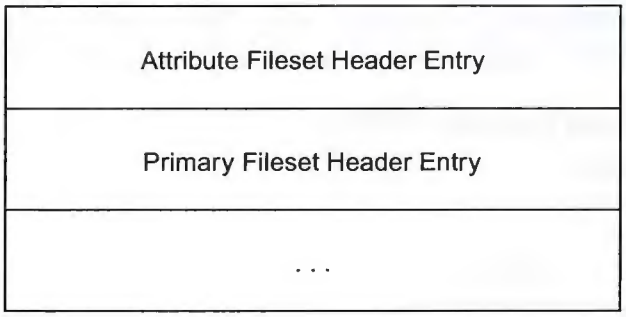
one fileset header per fileset (see Figure 2-6, "Fileset Header File"). Each fileset header entry is one block long. The fileset header file is replicated because fileset headers cannot be rebuilt from other data structures.

Figure 2-5 Filesets and Structural Files



RQS Nº 03/2005 - CN
CPMI - CORREIOS
1459
Fls:
Doc: 3701

Figure 2-6 **Fileset Header File**



The fileset header for a given fileset includes information such as:

- the fileset index (1 for the attribute fileset and 999 for the primary fileset)
- the fileset name
- the inode numbers of the fileset's inode list file and its replica
- the total number of allocated inodes
- the maximum number of inodes allowed in the fileset
- the inode list extent size (in blocks)
- the inode number of the file containing the inode allocation units for the fileset
- the inode number of the fileset's link count table (attribute fileset only)
- the inode number of the fileset's quotas file (primary fileset only)

Inodes

An inode is a data structure that contains information about a file. The VxFS inode size is 256 bytes. Each inode stores information about a particular file such as:

- file length
- link count
- owner and group IDs
- access privileges

E C T
4849

- time of last access
- time of last modification
- pointers to the extents that contain the file's data

There are up to ten direct extent address size pairs per inode. Each direct extent address indicates the starting block number of a direct extent; direct extent sizes can vary. If all of the direct extents are used, two indirect address extents are available for use in each inode. The first indirect address extent is used for single indirection, where each entry in the extent indicates the starting block number of an indirect data extent. The second indirect address extent is used for double indirection, where each entry in the extent indicates the starting block number of a single indirect address extent. Each indirect address extent is 8K long and contains 2048 entries. All indirect data extents for a given file have the same size, which is determined when the file's first indirect data extent is allocated.

Version 2 inodes differ from Version 1 inodes in that they are located in structural files to facilitate *dynamic inode allocation*, which is the allocation of inodes on an as-needed basis. Instead of allocating a fixed number of inodes into the file system, `mkfs` allocates a minimum number of inodes. Additional inodes are later allocated as the file system needs them.

The *inode list* is a series of inodes located in the inode list file. There is one inode in the list for every file in a given fileset. For recovery purposes, the inode list file is referenced by two inodes that point to the *same* set of data blocks. Although the inode addresses are replicated for recovery purposes, the inodes themselves are not.

An *inode extent* is an extent that contains inodes and is 8K long, by default. Inode extents are dynamically allocated to store inodes as they are needed.

Initial Inode List Extents The initial inode list extents contain the inodes first allocated by `mkfs_vxfs(1M)` for each fileset in a file system. During file system use, inodes are allocated as needed and are added into the inode list files for the filesets.

Figure 2-7, "Inode Lists" shows the initial inode list extents allocated for the primary and attribute filesets. Each of these extents contain 32 inodes and is 8K long.

The construction of the primary fileset's inode list resembles that of the

ROS Nº 03/2005 - CN
CPMI - CORREIOS
1460
Fls:
Doc:
3701

ECT
CPL - AC

VxFS Version 1 file system layout, with the first two inodes reserved and inodes 2 and 3 pre-assigned to the `root` and `lost+found` directories. The structural fileset's inode list is similarly constructed, with certain inodes allocated for specific files and other inodes reserved or unallocated.

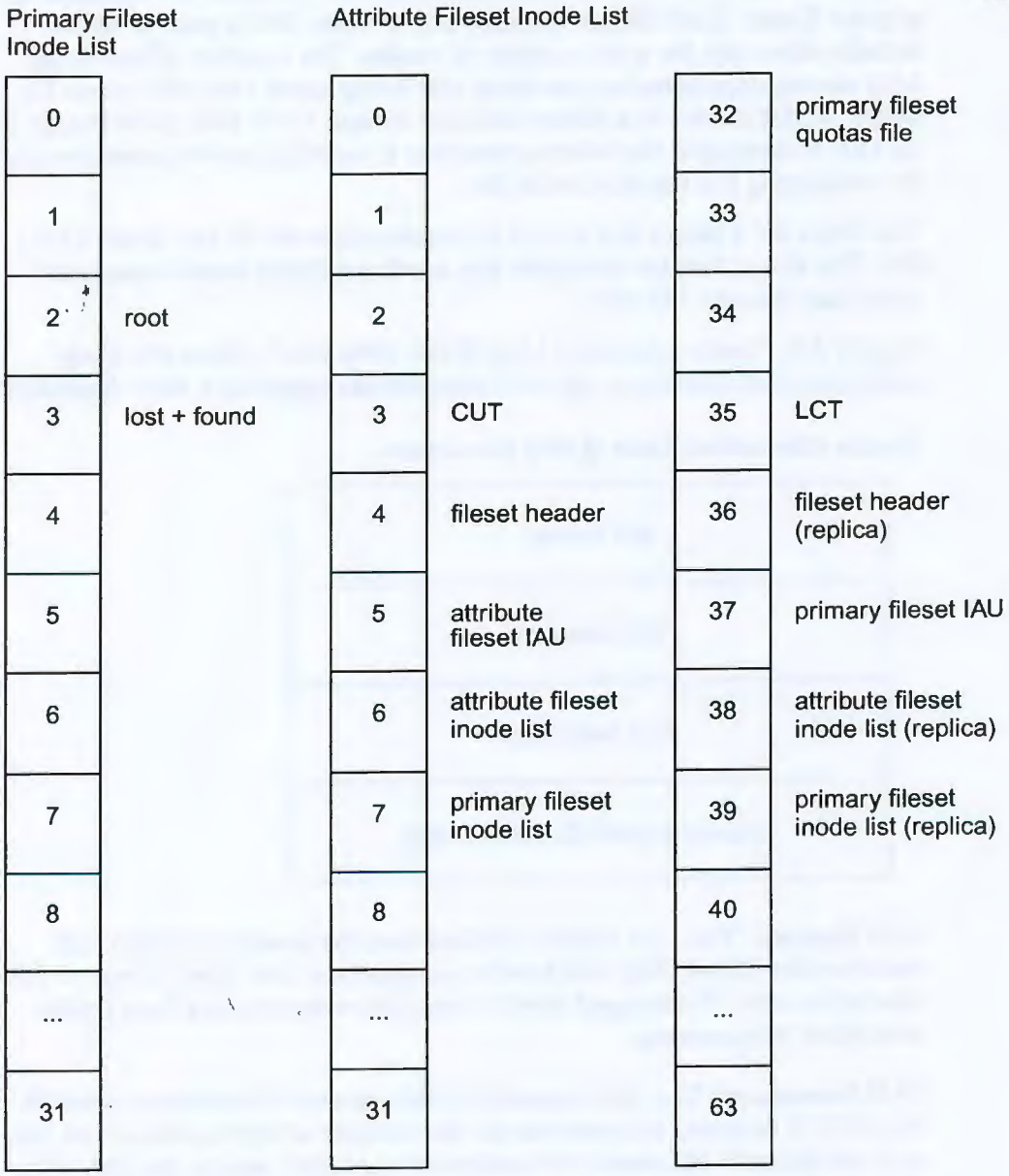
There are two initial inode list extents for the attribute fileset. These contain the inodes for all structural files needed to find and set up the file system.

Some of the entries in the structural fileset's inode list are replicas of one another. For example, inodes 4 and 36 both reference copies of the fileset header file. The replicated inodes are used by `fsck_vxfs(1M)` to reconstruct the file system in the event of damage to either one of the replicas. Although the two initial inode list extents belonging to the attribute fileset are logically contiguous, they are physically separated. This helps to ensure the integrity of the replicated information and reduces the chance that localized disk damage might result in complete loss of the file system.

Note that inodes 6 and 38 in the attribute fileset reference the inode list file for the attribute fileset. In a newly created file system, this file contains the two inode extents pictured for the attribute fileset. Likewise, the attribute fileset inodes 7 and 39 reference the inode list file for the primary fileset. In a newly created file system, this file contains the single extent pictured for the primary fileset. All of the unused inodes in the initial extents of the structural inode list are reserved for future use.

E C
4847
Paula
AC

Figure 2-7 Inode Lists



RQS Nº 03/2005 - CN
CPMI - CORREIOS
1461
Fls:
3701
Doc:

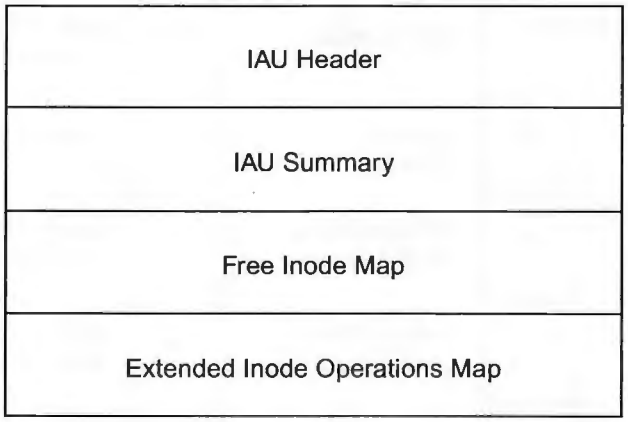
Inode Allocation Unit

An Inode Allocation Unit (IAU) contains inode allocation information for a given fileset. Each fileset contains one or more IAUs, each of which details allocation for a set number of inodes. The number of inodes per IAU varies, depending on the block size being used. One IAU exists for every 16,384 inodes in a fileset with the default block size (1024 bytes). If an IAU is damaged, the information that it contains can be reconstructed by examining the fileset's inode list.

The IAUs for a fileset are stored in sequential order in the fileset's IAU file. The fileset header identifies the attribute fileset inode associated with that fileset's IAU file.

Figure 2-8, "Inode Allocation Unit (IAU) Structure" shows the inode allocation unit structure. All IAU components begin on a block boundary.

Figure 2-8 **Inode Allocation Unit (IAU) Structure**



IAU Header The IAU header verifies that the inode allocation unit matches the fileset. The IAU header occupies the first block of each inode allocation unit. If damaged, the IAU can be reconstructed from inodes and other information.

IAU Summary The IAU summary summarizes the resources used in the IAU. It includes information on the number of free inodes in the IAU and the number of inodes with extended operation sets in the IAU. The IAU summary is 1 block long.

Free Inode Map The free inode map is a bitmap that indicates which inodes are free and which are allocated. A free inode is indicated by the

bit being on. The length of the free inode map is 2K for file systems with 1K or 2K block sizes and is equal to the block size for file systems with larger block sizes.

Extended Inode Operations Map The extended inode operations map keeps track of inodes on which operations would remain pending for too long to reside in the intent log. The extended inode operations map is in the same format as the free inode map. To prevent the intent log from wrapping and the transaction from getting overwritten, the required operations are stored in the affected inode. This map is then updated to identify the inodes that have extended operations that need to be completed. This map allows the `fsck` utility to quickly identify which inodes had extended operations pending at the time of a system failure. The length of the extended inode operations map is 2K for file systems with 1K or 2K block sizes and is equal to the block size for file systems with larger block sizes.

Link Count Table

The link count table (LCT) contains a reference count for each inode in the associated fileset. This reference count is identical to the conventional link field of an inode. Each LCT entry contains the actual reference count for the associated fileset inode. The link count field in an inode itself is set to either 0 or 1, and the actual number of links is stored in the LCT entry for the associated fileset inode.

The link count table can be reconstructed using the inode list, so it is not replicated.

The current layout only uses the LCT for inodes in the attribute fileset. The LCT supports quick updates of the link count for structural fileset inodes.

Current Usage Table

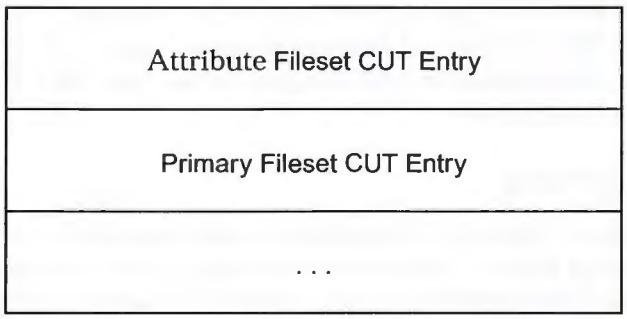
The current usage table (CUT) is a file that contains usage related information for each fileset. The information contained in the CUT changes frequently and is not replicated. The information in the CUT can, however, be reconstructed using the inode list if the CUT is damaged.

The CUT file contains one entry per fileset (see Figure 2-9, "Current Usage Table (CUT) File"). The CUT entry for a given fileset contains information such as the following:

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1462
Fls:
Doc: 3701

- The number of blocks currently used by the fileset.
- The *fileset version number*, which is a 64-bit integer that is guaranteed to be at least as large as the largest inode version number. An *inode version number* is a 64-bit integer that is incremented every time its inode is modified or written to disk and can be used to indicate whether an inode has been modified in any way since the last time it was examined. It is possible to find out which inodes have been modified since a specific time by saving the fileset version number and then later looking for inodes with a larger version number.

Figure 2-9 **Current Usage Table (CUT) File**



Quotas File

VxFS supports BSD-style quotas for users. Quota information is stored in a quotas file. A user quotas file tracks the resources used by each user ID. The quotas file keeps track of soft limits, hard limits, block usage, and inode usage for users within a file system.

Because quotas apply to mountable filesets only, the attribute fileset does not have quotas. However, the primary fileset's quotas file exists as a structural file in the attribute fileset. The primary fileset's user quotas file is referenced by the structural fileset's initial inode list extent.

Locating Dynamic Structures

The existence of dynamic structures in the Version 2 disk layout makes the task of initially locating those structures difficult. The object location table (OLT) contains information needed to initially locate important file system structural elements. In particular, the OLT records the starting

block numbers of the initial inode list extents for the attribute fileset and indicates which inodes within those initial extents reference the fileset header file.

Object Location Table Contents

The OLT is composed of records for the following:

fileset header inodes	This record identifies the inode numbers of the fileset header file and its replica.
initial inode list extent addresses	This record identifies the addresses of the beginning of each of two 8K inode extents. These are the initial inode list extents for the attribute fileset, which contain the inodes for all structural files belonging to the attribute fileset.
current usage table inode	This record identifies the inode number of the file that contains the current usage table.

Mounting and the Object Location Table

At mount time, the object location table provides essential information about the location of key file system components. The super-block plays an important role in locating the OLT, in that it contains pointers to both the OLT and its replica.

Using the OLT, the process of mounting a VxFS Version 2 file system is:

Step 1. Read in the super-block. Validate the super-block and its replicas (located in the allocation unit headers).

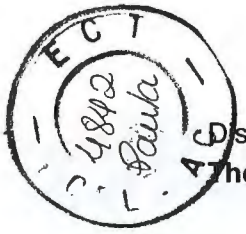
Step 2. Read and validate the OLT and its replica at the locations recorded in the super-block.

Step 3. Obtain the addresses of the initial inode list extents for the attribute fileset from the OLT. Read in these initial inode extents.

Step 4. Find the fileset header file, based on the fileset header file inode number recorded in the OLT.

Step 5. Read the contents of the fileset header file. Each fileset header file entry represents a particular fileset and indicates the inode numbers of its inode list file and IAU file. The attribute fileset is set up first so that subsequent references to its inode list can be resolved.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1463
Doc:
3701



The VxFS Version 3 Disk Layout

The Version 3 disk layout allows the file system to scale easily to accommodate large files and large file systems.

The Version 1 and 2 disk layouts divided up the file system space into allocation units. The first AU started part way into the file system which caused potential alignment problems depending on where the first AU started. Each allocation unit also had its own summary, bitmaps, and data blocks. Because this AU structural information was stored at the start of each AU, this also limited the maximum size of an extent that could be allocated. By replacing the allocation unit model of previous versions, the need for alignment of allocation units and the restriction on extent sizes was removed.

The VxFS Version 3 disk layout divides the entire file system space into fixed size allocation units. The first allocation unit starts at block zero and all allocation units are a fixed length of 32K blocks. (An exception may be the last AU, which occupies whatever space remains at the end of the file system). Because the first AU starts at block zero instead of part way through the file system as in previous versions, there is no longer a need for explicit AU alignment or padding to be added when creating a file system (see `mkfs_vxfs`(1M)).

The Version 3 file system also moves away from the model of storing AU structural data at the start of an AU and puts all structural information in files. So expanding the file system structures simply requires extending the appropriate structural files. This removes the extent size restriction imposed by the Version 1 and Version 2 layouts.

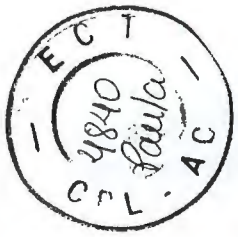
All Version 3 structural files reside in the *`structural fileset`*, which is similar to the Version 2 attribute fileset. The structural files in the Version 3 disk layout are:

object location table file	Contains the object location table (OLT). As with the Version 2 disk layout, the OLT, which is referenced from the super-block, is used to locate the other structural files.
label file	Encapsulates the super-block and super-block replicas. Although the location of the primary super-block is

E 4841 Paulo

	known, the label file can be used to locate super-block copies if there is structural damage to the file system.
device file	Records device information such as volume length and volume label, and contains pointers to other structural files.
fileset header file	Holds information on a per-fileset basis. This may include the inode of the fileset's inode list file, the maximum number of inodes allowed, an indication of whether the file system supports large files, and the inode number of the quotas file if the fileset supports quotas. When a file system is created, there are two filesets—the *structural fileset* defines the file system structure, the *primary fileset* contains user data.
inode list file	Both the primary fileset and the structural fileset have their own set of inodes stored in an inode list file. Only the inodes in the primary fileset are visible to users. When the number of inodes is increased, the kernel increases the size of the inode list file.
inode allocation unit file	Holds the free inode map, extended operations map, and a summary of inode resources.
log file	Maps the block used by the file system intent log.
extent allocation unit state file	Indicates the allocation state of each AU by defining whether each AU is free, allocated as a whole (no bitmaps allocated), or expanded, in which case the bitmaps associated with each AU determine which extents are

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1464
Fls:
Doc: 3701



	allocated.
extent allocation unit summary file	Contains the AU summary for each allocation unit, which contains the number of free extents of each size. The summary for an extent is created only when an allocation unit is expanded for use.
free extent map file	Contains the free extent maps for each of the allocation units.
quotas file	If the file system supports quotas, there is a quotas file which is used to track the resources allocated to each user.

Figure 2-10, "VxFS Version 3 Disk Layout" shows how the kernel and utilities build information about the structure of the file system. The super-block location is in a known location from which the OLT can be located. From the OLT, the initial extents of the structural inode list can be located along with the inode number of the fileset header file. The initial inode list extents contain the inode for the fileset header file from which the extents associated with the fileset header file are obtained.

As an example, when mounting the file system, the kernel needs to access the primary fileset in order to access its inode list, inode allocation unit, quotas file and so on. The required information is obtained by accessing the fileset header file from which the kernel can locate the appropriate entry in the file and access the required information.

E C T
24834
Paulo
A C

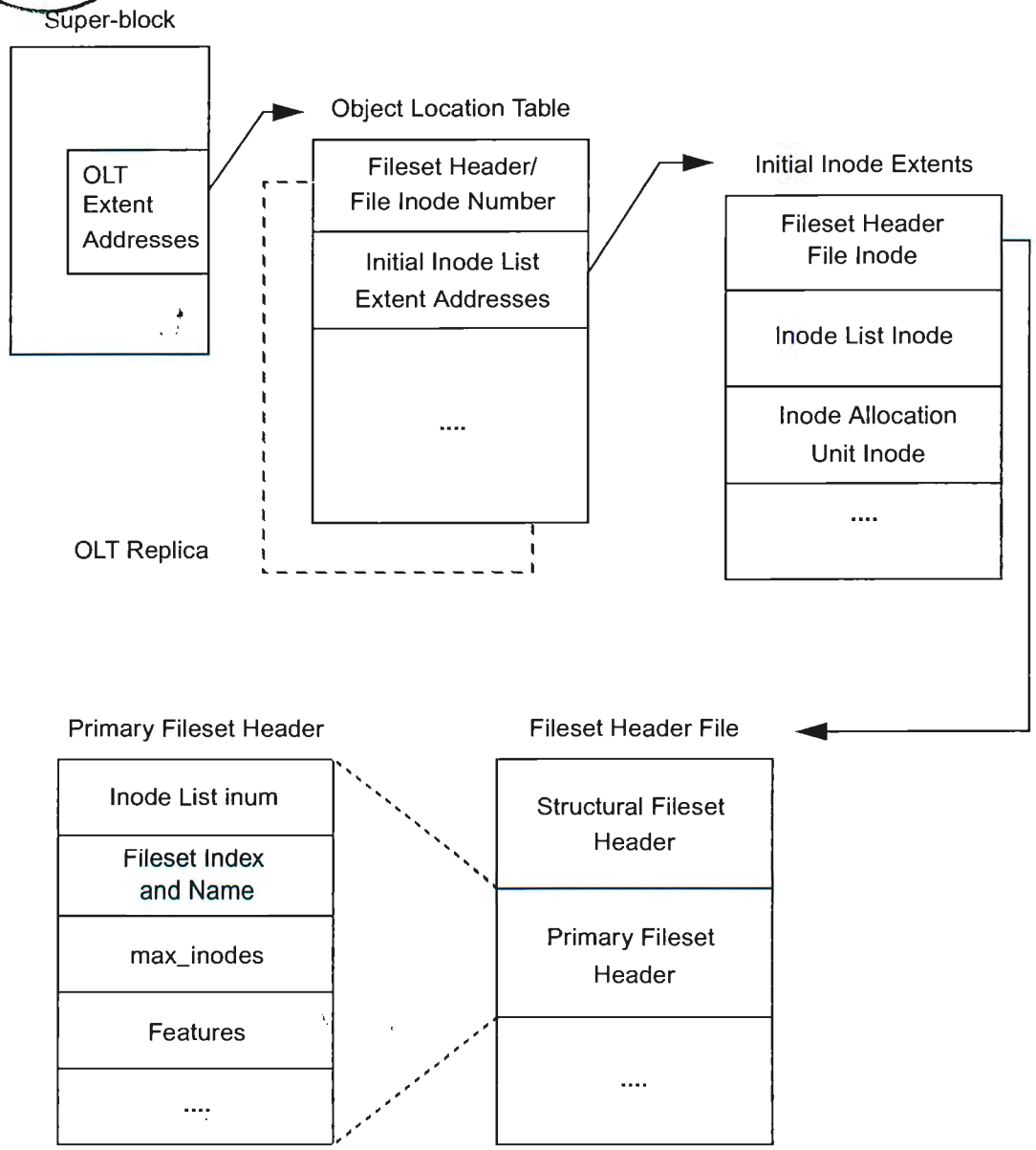
The VxFS Version 4 Disk Layout

The Version 4 disk layout supports Access Control Lists.

The Version 4 disk layout does not include significant physical changes from the Version 3 disk layout. Instead, the policies implemented for Version 4 are different, allowing for performance improvements, file system shrinking, and other enhancements.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1465
Doc: 3701

Figure 2-10 **VxFS Version 3 Disk Layout**



Extent Attributes
4834
Paula
AC

3 Extent Attributes

ROS Nº 03/2005 - CN
CPMI - CORREIOS
1466
Fls:
Doc: 3701

ECT 1836 Paulo CPL - AC

Introduction

The VxFS file system allocates disk space to files in groups of one or more adjacent blocks called *extents*. VxFS defines an application interface that allows programs to control various aspects of the extent allocation for a given file (see Chapter 6 , "Application Interface"). The extent allocation policies associated with a file are referred to as *extent attributes*.

The VxFS `getext` and `setext` commands allows users to view or manipulate file extent attributes. In addition, the `vxdump`, `vxrestore`, `mv`, `cp`, and `cpio` commands preserve extent attributes when a file is backed up, moved, copied, or archived.

NOTE

`setext` functionality is available only with the optional HP OnLineJFS product.

The following topics are covered in this chapter:

- "Attribute Specifics"
  - — "Reservation: Preallocating Space to a File"
  - — "Fixed Extent Size"
  - — "Other Controls"
- "Commands Related to Extent Attributes"
  - — "Failure to Preserve Extent Attributes"

Attribute Specifics

The two basic extent attributes associated with a file are its *reservation* and its *fixed extent size*. The user can preallocate space to the file by manipulating a file's reservation; the user can also override the default allocation policy of the file system by setting a fixed extent size.

Other policies determine the way these attributes are expressed during the allocation process. The user can specify that:

- the space reserved for a file must be contiguous
- no allocations should be made for a file beyond the current reservation
- unused reservation should be released when the file is closed
- space should be allocated but no reservation should be assigned
- the file size should be changed to immediately incorporate the allocated space

Some of the extent attributes are persistent and become part of the on-disk information about the file, while other attributes are temporary and lost after the file is closed or the system is rebooted. The persistent attributes are similar to the file's permissions and are actually written in the inode for the file. When a file is copied, moved, or archived, only the persistent attributes of the source file can be preserved in the new file (see "Other Controls" for more information).

In general, the user will only set extent attributes for reservation. Many of the attributes are designed for applications that are tuned to a particular pattern of I/O or disk alignment (see `mkfs_vxfs`(1M) and Chapter 6., "Application Interface" for more information).

Reservation: Preallocating Space to a File

VxFS makes it possible to preallocate space to a file at the time of the request rather than when data is written into the file. This space cannot be allocated to other files in the file system. VxFS prevents any unexpected out-of-space condition on the file system by ensuring that a file's required space will be associated with the file before it is required.

ROS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1467
Doc: 3701

Persistent reservation is not released when a file is truncated. The reservation must be cleared or the file must be removed to free reserved space.

Fixed Extent Size

The VxFS default allocation policy uses a variety of heuristics to determine how to make an allocation to a file when a write requires additional space. The policy attempts to balance the two goals of optimum I/O performance through large allocations and minimal file system fragmentation through allocation from space available in the file system that best fits the data.

Setting a fixed extent size overrides the default allocation policies for a file and always serves as a persistent attribute. Be careful to choose an extent size appropriate to the application when using fixed extents. An advantage of VxFS's extent based allocation policies is that they rarely use indirect blocks compared to block based file systems; VxFS eliminates many instances of disk access that stem from indirect references. However, a small extent size can eliminate this advantage.

Files with aggressive allocation sizes tend to be more contiguous and have better I/O characteristics. However, the overall performance of the file system degrades because the unused space fragments free space by breaking large extents into smaller pieces. By erring on the side of minimizing fragmentation for the file system, files may become so non-contiguous that their I/O characteristics would degrade.

Fixed extent sizes are particularly appropriate in the following situations:

- If a file is large and sparse and its write size is fixed, a fixed extent size that is a multiple of the write size can minimize space wasted by blocks that do not contain user data as a result of misalignment of write and extent sizes. (The default extent size for a sparse file is 8K.)
- If a file is large and contiguous, a large fixed extent size can minimize the number of extents in the file.

Custom applications may also use fixed extent sizes for specific reasons, such as the need to align extents to cylinder or striping boundaries on disk.

Other Controls

The auxiliary controls on extent attributes determine:

- whether allocations are aligned
- whether allocations are contiguous
- whether the file can be written beyond its reservation
- whether an unused reservation is released when the file is closed
- whether the reservation is a persistent attribute of the file
- when the space reserved for a file will actually become part of the file

Alignment

Specific alignment restrictions coordinate a file's allocations with a particular I/O pattern or disk alignment (see `mkfs_vxfs`(1M) and Chapter 6 , "Application Interface" for details). Alignment can only be specified if a fixed extent size has also been set. Setting alignment restrictions on allocations is best left to well designed applications.

Contiguity

A reservation request can specify that its allocation remain contiguous (all one extent). Maximum contiguity of a file optimizes its I/O characteristics.

NOTE

Fixed extent sizes or alignment will cause the file system to return an error message reporting insufficient space if no suitably sized (or aligned) extent is available. This may happen even if the file system has plenty of free space and the fixed extent size is large.

Write Operations Beyond Reservation

A reservation request can specify that no allocations can take place after a write operation fills up the last available block in the reservation. This specification can be used in a similar way to `ulimit` to prevent a file's uncontrolled growth.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1468
Fls:
3701
Doc:

Reservation Trimming

A reservation request can specify that any unused reservation be released when the file is closed. The file is not completely closed until all processes open against the file have closed it.

Reservation Persistence

A reservation request can ensure the reservation does not become a persistent attribute of the file. Unused reservation is discarded when the file is closed.

Including Reservation in the File

A reservation request can make sure the size of the file is adjusted to include the reservation. Normally, the space of the reservation is not included in the file until an extending write operation requires it. A reservation that immediately changes the file size can generate large temporary files. Unlike a `ftruncate` operation that increases the size of a file, this type of reservation does not perform zeroing of the blocks included in the file and limits this facility to users with appropriate privileges. The data that appears in the file may have been previously contained in another file.

E 482/C Paula
L - AC

Commands Related to Extent Attributes

The VxFS commands for manipulating extent attributes are `setext` and `getext`; they allow the user to set up files with a given set of extent attributes or view any attributes that are already associated with a file. See `getext`(1M) and `setext`(1M) for details on using these commands.

NOTE `setext` functionality is available only with the optional HP OnLineJFS product.

The VxFS-specific commands `vxdump` and `vxrestore`, and the `mv`, `cp`, and `cpio` commands, preserve extent attributes when backing up, restoring, moving, or copying files.

Most of these commands include a command line option (`-e`) for maintaining extent attributes on files. This option specifies dealing with a VxFS file that has extent attribute information including reserved space, a fixed extent size, and extent alignment. The extent attribute information may be lost if the destination file system does not support extent attributes, has a different block size than the source file system, or lacks free extents appropriate to satisfy the extent attribute requirements.

The `-e` option takes any of the following keywords as an argument:

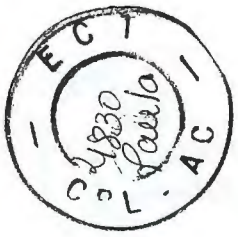
`warn`	Issues a warning message if extent attribute information cannot be maintained (the default)
`force`	Fails the copy if extent attribute information cannot be maintained
`ignore`	Ignores extent attribute information entirely

The commands that move, copy, or archive files (`mv`, `cp` and `cpio`) use the `-e` option with arguments of `ignore`, `warn`, or `force`.

For example, the `mv` command could be used with the `-e` option to produce the following results:

- The `ignore` keyword loses any extent attributes for files.
- The `warn` keyword issues a warning if extent attributes for a file cannot be preserved. Such a situation may take place if the file is moved into a non-VxFS file system; the file would ultimately be moved while the extent attributes would be lost.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1469
Fls:
Doc: 3701



- The `force` keyword issues an error if attributes are lost and the file is not relocated.

  The `ls` command has an `-e` option, which prints the extent attributes of the file.

Failure to Preserve Extent Attributes

Whenever a file is copied, moved, or archived using commands that preserve extent attributes, there is nevertheless the possibility of losing the attributes. Such a failure might occur for three reasons:

- The file system receiving a copied, moved, or restored file from an archive is not a VxFS type. Since other file system types do not support the extent attributes of the VxFS file system, the attributes of the source file are lost during the migration.
- The file system receiving a copied, moved, or restored file is a VxFS type but does not have enough free space to satisfy the extent attributes. For example, consider a 50K file and a reservation of 1 MB. If the target file system has 500K free, it could easily hold the file but fail to satisfy the reservation.
- The file system receiving a copied, moved, or restored file from an archive is a VxFS type but the different block sizes of the source and target file system make extent attributes impossible to maintain. For example, consider a source file system of block size 1024, a target file system of block size 4096, and a file that has a fixed extent size of 3 blocks (3072 bytes). This fixed extent size adapts to the source file system but cannot translate onto the target file system.

The same source and target file systems in the preceding example with a file carrying a fixed extent size of 4 could preserve the attribute; a 4 block (4096 byte) extent on the source file system would translate into a 1 block extent on the target.

On a system with mixed block sizes, a copy, move, or restoration operation may or may not succeed in preserving attributes. It is recommended that the same block size be used for all file systems on a given system.

1478 Fls. CPL - AC

Electrical Factors

Proper design and installation of a power distribution system for a Superdome server requires specialized skills. Those responsible for this task must have a thorough knowledge and understanding of appropriate electrical codes and the limitations of the power systems for computer and data processing equipment.

In general, a well-designed power distribution system exceeds the requirements of most electrical codes. A good design, when coupled with proper installation practices, produces the most trouble-free operation.

A detailed discussion of power distribution system design and installation is beyond the scope of this document. However, electrical factors relating to power distribution system design and installation must be considered during the site preparation process.

The electrical factors discussed in this section are:

- Computer room safety
- Electrical load requirements (circuit breaker sizing)
- Power quality
- Distribution hardware
- System installation guidelines

Computer Room Safety

Inside the computer room, fire protection and adequate lighting (for equipment servicing) are important safety considerations. Federal and local safety codes govern computer installations.

Fire Protection

The National Fire Protection Association's Standard for the Protection of Electronic Computer Data Processing Equipment, NFPA 75, contains information on safety monitoring equipment for computer rooms.

Most computer room installations are equipped with the following fire protection devices:

- Smoke detectors
- Fire and temperature alarms
- Fire extinguishing system

Additional safety devices are:

- Circuit breakers
- An emergency power cutoff switch
- Devices specific to the geographic location, i.e., earthquake protection

Lighting Requirements for Equipment Servicing

Adequate lighting and utility outlets in a computer room reduce the possibility of accidents during equipment servicing. Safer servicing is also more efficient and, therefore, less costly.

For example, it is difficult to see cable connection points on the hardware if there is not enough light. Adequate lighting reduces the chances of connector damage when cables are installed or removed.

ECT Nº 03/2005 - CN
CPMI - CORREIOS
1470
Fls:
Doc: 3701

The minimum recommended illumination level is 70 foot-candles (756 lumens per square meter) when the light level is measured at 30 inches (76.2 cm) above the floor.

Power Quality

This equipment is designed to operate over a wide range of voltages and frequencies. It has been tested and shown to comply with EMC Specification EN50082. However, damage can occur if these ranges are exceeded. Severe electrical disturbances can exceed the design specifications of the equipment.

Sources of Electrical Disturbances

Electrical disturbances, glitches, affect the quality of electrical power. Common sources of these disturbances are:

- Fluctuations occurring within the facility's distribution system
- Utility service low-voltage conditions (such as sags or brownouts)
- Wide and rapid variations in input voltage levels
- Wide and rapid variations in input power frequency
- Electrical storms
- Large inductive sources (such as motors and welders)
- Faults in the distribution system wiring (such as loose connections)
- Microwave, radar, radio, or cell phone transmissions

Power System Protection

Computer systems can be protected from the sources of many of these electrical disturbances by using:

- A Protective Earth (PE) connection with a wire diameter of at least equal to the current carrying conductors. The neutral conductor must not be used for the PE connection. (The PE wire is GREEN with a YELLOW stripe.)
- A dedicated power distribution system
- Power conditioning equipment
- Over- and under-voltage detection and protection circuits
- Screening to cancel out the effects of undesirable transmissions
- Lightning arresters on power cables to protect equipment against electrical storms

Every precaution has been taken during power distribution system design to provide immunity to power outages of less than one cycle. However, testing cannot conclusively rule out loss of service. Therefore, adherence to the following guidelines provides the best possible performance of power distribution systems for Superdome server equipment:

- Dedicated power source—Isolates server power distribution system from other circuits in the facility.
- Missing-phase and low-voltage detectors—Shuts equipment down automatically when a severe power disruption occurs. For peripheral equipment, these devices are recommended but optional.
- Online uninterruptable power supply (UPS)—Keeps input voltage to devices constant and should be considered if outages of one-half cycle or more are common. Refer to qualified contractors or consultants for each situation.

4976 Paula

Distribution Hardware

This section describes wire selection and the types of raceways (electrical conduits) used in the distribution system. Wire size is dictated by circuit breaker sizing and local safety codes.

Wire Selection

Use copper conductors instead of aluminum, as aluminum's coefficient of expansion differs significantly from that of other metals used in power hardware. Because of this difference, aluminum conductors can cause connector hardware to work loose, overheat, and fail.

Raceway Systems (Electrical Conduits)

Raceways (electrical conduits) form part of the protective ground path for personnel and equipment. Raceways protect the wiring from accidental damage and also provide a heat sink for the wires.

Any of the following types may be used:

- Electrical metallic tubing (EMT) thin-wall tubing
- Rigid (metal) conduit
- Liquidtight with RFI strain relief (most commonly used with raised floors)
- Plenum-grade cables

Building Distribution

All building feeders and branch circuitry should be in rigid metallic conduit with proper connectors (to provide ground continuity). Conduit that is exposed and subject to damage should be constructed of rigid galvanized steel.

The IOX and Superdome are safety grounded through the green (ground) wire in each AC power cord. In the IOX, this ground passes through the AC power cord entry into the XPC and connects internally to the XPC chassis. The XUC chassis and each ICE chassis are grounded through their respective DC power cords from the XPC. Additional safety grounding must be provided for networking equipment.

Power Routing

Power drops and interface cables from the equipment are routed down from the power panel, through a grommet-protected opening (beneath the floor level), and under the floor panels.

Grounding Systems

Superdome servers require two methods of grounding:

- Power distribution safety grounding
- High frequency intercabinet grounding

Power Distribution Safety Grounding

The power distribution safety grounding system consists of connecting various points in the power distribution system to earth ground using green (green/yellow) wire ground conductors. Having these ground connections tied to metal chassis parts that may be touched protects computer room personnel against shock hazard from current leakage and fault conditions.

Power distribution systems consist of several parts. Hewlett-Packard recommends that these parts be solidly interconnected to provide an equipotential ground to all points.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1471
Fls:
Doc: 3791

Main Building Electrical Ground The main electrical service entrance equipment should have an earth ground connection, as required by applicable codes. Connections such as a grounding rod, building steel, or a conductive type cold water service pipe provide an earth ground.

Electrical Conduit Ground To provide a continuous grounding system, all electrical conduits should be made of rigid metallic conduit that is securely connected together or bonded to panels and electrical boxes.

Power Panel Ground Each power panel should be grounded to the electrical service entrance with green (green/yellow) wire ground conductors. The green (green/yellow) wire ground conductors should be sized per applicable codes (based on circuit over current device ratings).

NOTE The green wire ground conductor mentioned above may be a black wire marked with green tape.

Computer Safety Ground Ground all computer equipment with the green (green/yellow) wire included in the branch circuitry. The green (green/yellow) wire ground conductors should be connected to the appropriate power panel and should be sized per applicable codes (based on circuit over current device ratings).

Superdome was approved by regulatory agencies around the world, and therefore requires a ground/protective earth. there are no exclusions to this regulatory approval.

High-frequency grounding between IOX and Superdome is provided by the cabinet-to-cabinet signal cabling. Whenever an IOX is connected to a Superdome cabinet, low-frequency grounding between these two cabinets is provided by a ground strap. This ground strap is shipped with each IOX. Refer to the *I/O Expansion Cabinet Guide* for more detail.

Newtwork-connected Equipment Ground The installation must provide a ground connection for the network equipment. This statement is translated into the following two languages as required:

WARNING **Sweden: Apparaten skall anslutas till jordat uttag, när den ansluts till ett nätverk.**

WARNING **Denmark: Før tilslutning af de øvrige ledere, se medfølgende installationsvejledning.**

System Installation Guidelines

This section contains information about installation practices. Some common pitfalls are highlighted. Both power cable and data communications cable installations are discussed.

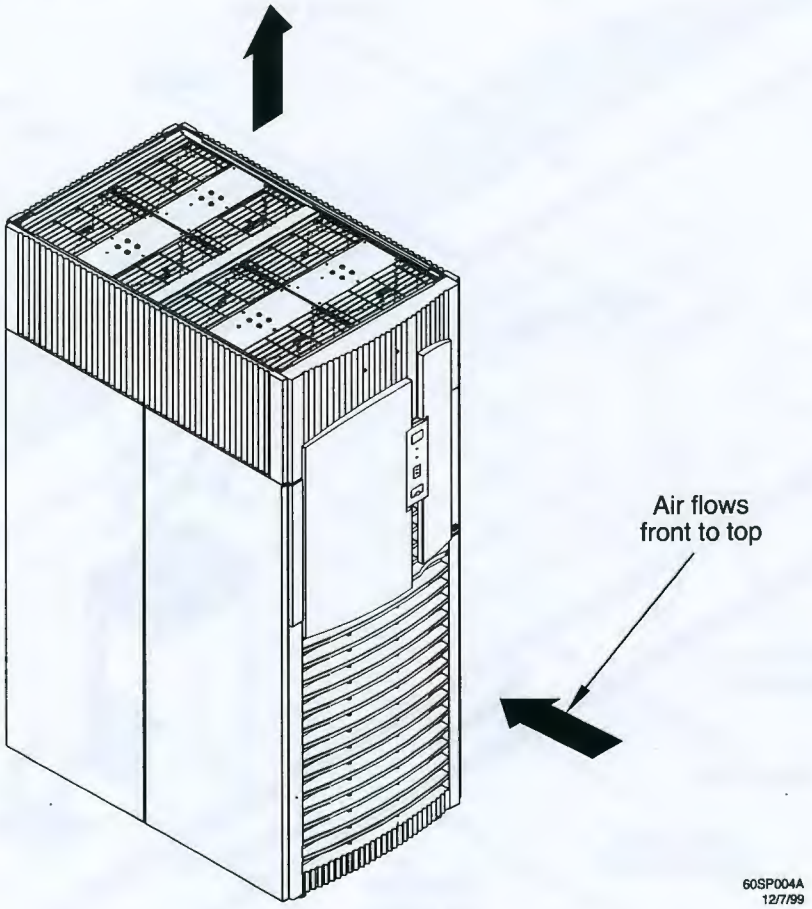
Wiring Connections

Expansion and contraction rates vary among different metals. Therefore, the integrity of an electrical connection depends on the restraining force applied. Connections that are too tight compress or deform the hardware and causes it to weaken. This usually leads to high impedance causing circuit breakers to trip.

CAUTION Connections that are too loose have a high resistance that cause serious problems, such as erratic equipment operation. A high resistance connection overheats and sometimes causes fire or high temperatures that can destroy hard-to-replace components such as distribution panels or system bus bars.

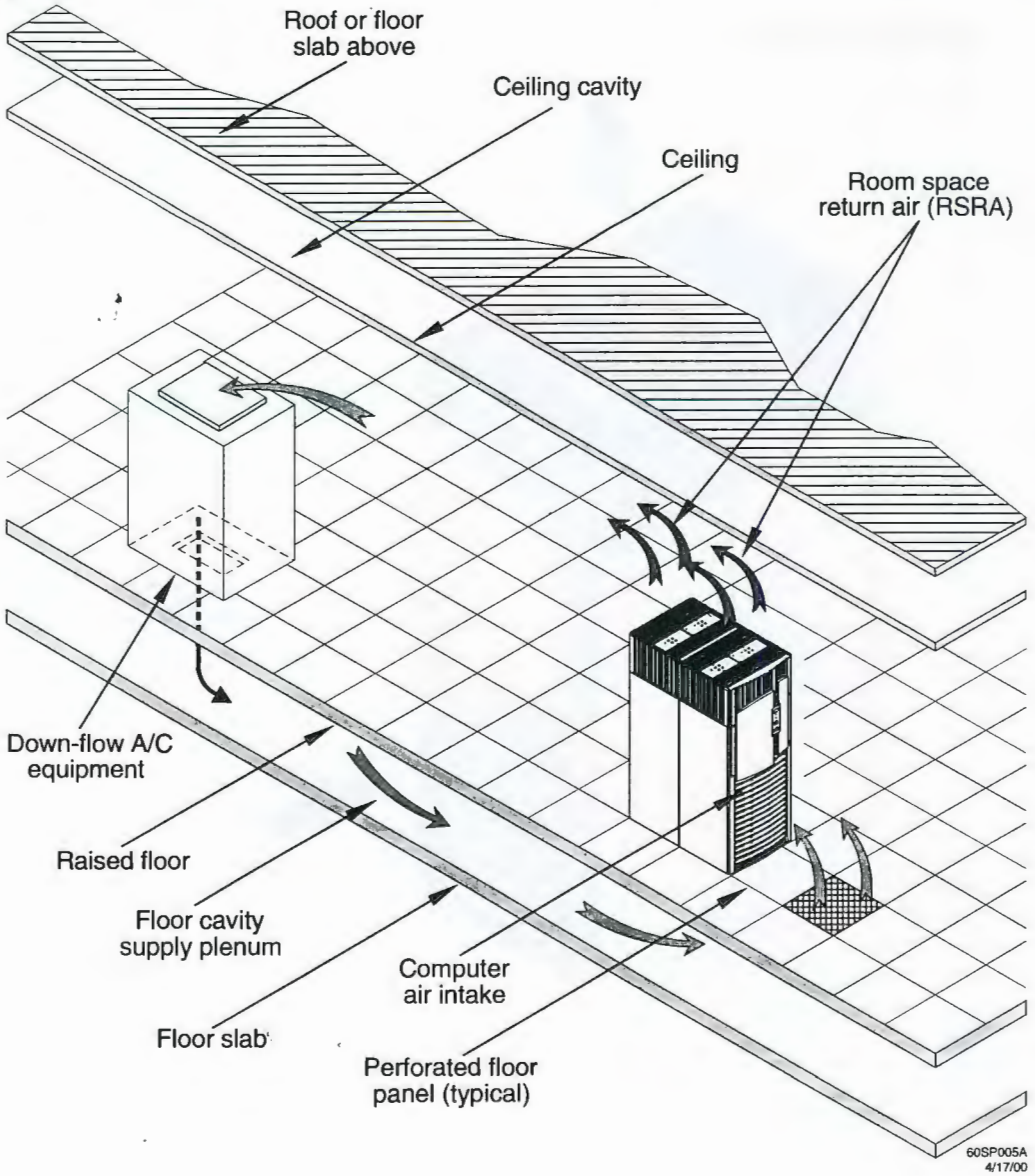
Figure 1-17 on page 34 through Figure 1-19 on page 36 illustrate typical cooling system layouts, adapted from the typical cooling system described in Chapter 2.

Figure 1-16 Airflow Diagram



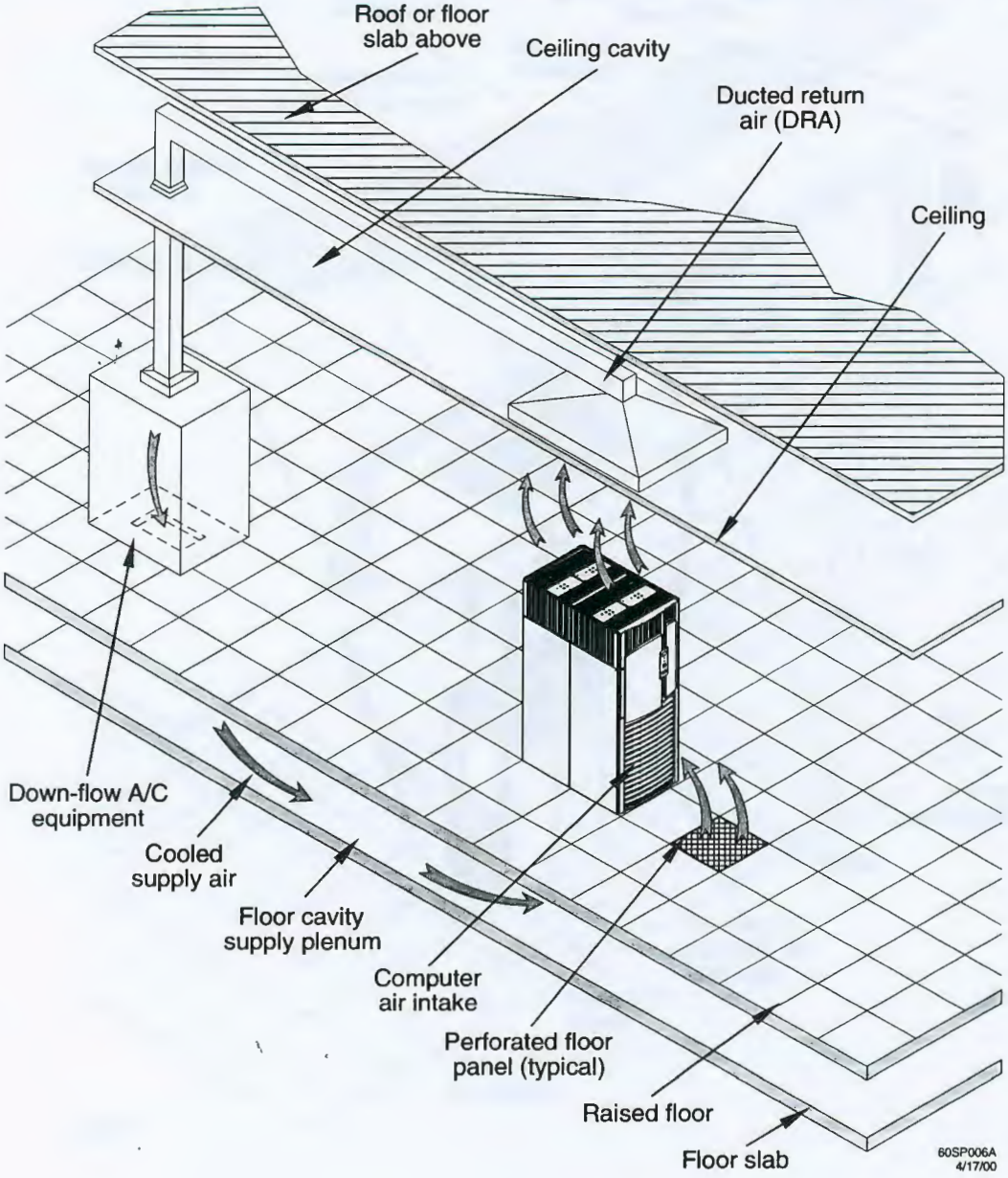
RQS Nº 03/2005 - CN
CPMI - CORREIOS
1472
Fls:
Doc: 3701

Figure 1-17 Typical Superdome Room Space Return Air Cooling System



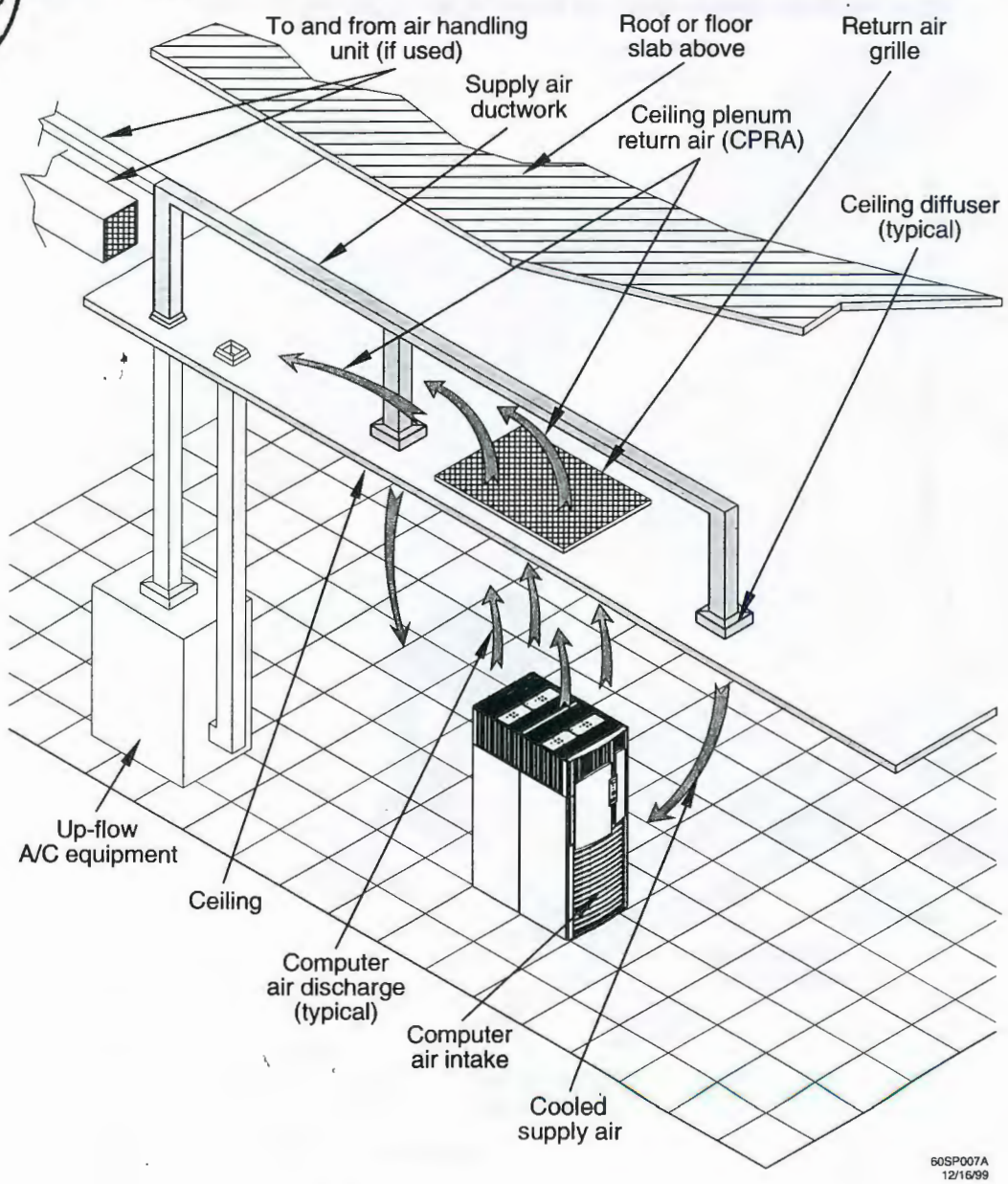
E C T
CPL - AC
1982

Figure 1-18 Typical Superdome Ducted Return Air Cooling System



RQS Nº 03/2005 - CN
CPMI - CORREIOS
1473
Fls:
Doc: 3701

Figure 1-19 Typical Superdome Ceiling Plenum Return Air Cooling System



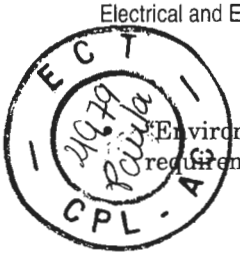
E C T
1980
Paula
CPL - AC

2 Electrical and Environmental Guidelines

This chapter provides guidelines for planning and preparing the site. Careful site planning and preparation ensures trouble-free installation and reliable operation of Superdome servers. Factors that may contribute to less than optimal equipment operation are also highlighted.

- "Electrical Factors" on page 39 discusses computer room safety, electrical load requirements, power quality, distribution hardware, and system installation guidelines.

PROAD 09/2005 - CN
CPMI - CORREIOS
Fls: 1474
3701
Doc: 37



"Environmental Elements" on page 44 discusses computer room preparation, cooling and humidity requirements, dust and pollution control, electrostatic discharge prevention, and acoustics.

3978
Paula
CPL - AC

Electrical Factors

Proper design and installation of a power distribution system for a Superdome server requires specialized skills. Those responsible for this task must have a thorough knowledge and understanding of appropriate electrical codes and the limitations of the power systems for computer and data processing equipment.

In general, a well-designed power distribution system exceeds the requirements of most electrical codes. A good design, when coupled with proper installation practices, produces the most trouble-free operation.

A detailed discussion of power distribution system design and installation is beyond the scope of this document. However, electrical factors relating to power distribution system design and installation must be considered during the site preparation process.

The electrical factors discussed in this section are:

- Computer room safety
- Electrical load requirements (circuit breaker sizing)
- Power quality
- Distribution hardware
- System installation guidelines

Computer Room Safety

Inside the computer room, fire protection and adequate lighting (for equipment servicing) are important safety considerations. Federal and local safety codes govern computer installations.

Fire Protection

The National Fire Protection Association's Standard for the Protection of Electronic Computer Data Processing Equipment, NFPA 75, contains information on safety monitoring equipment for computer rooms.

Most computer room installations are equipped with the following fire protection devices:

- Smoke detectors
- Fire and temperature alarms
- Fire extinguishing system

Additional safety devices are:

- Circuit breakers
- An emergency power cutoff switch
- Devices specific to the geographic location, i.e., earthquake protection

Lighting Requirements for Equipment Servicing

Adequate lighting and utility outlets in a computer room reduce the possibility of accidents during equipment servicing. Safer servicing is also more efficient and, therefore, less costly.

For example, it is difficult to see cable connection points on the hardware if there is not enough light. Adequate lighting reduces the chances of connector damage when cables are installed or removed.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1475
Fls:
Doc: 3701

The minimum recommended illumination level is 70 foot-candles (756 lumens per square meter) when the light level is measured at 30 inches (76.2 cm) above the floor.

Power Quality

This equipment is designed to operate over a wide range of voltages and frequencies. It has been tested and shown to comply with EMC Specification EN50082. However, damage can occur if these ranges are exceeded. Severe electrical disturbances can exceed the design specifications of the equipment.

Sources of Electrical Disturbances

Electrical disturbances, glitches, affect the quality of electrical power. Common sources of these disturbances are:

- Fluctuations occurring within the facility's distribution system
- Utility service low-voltage conditions (such as sags or brownouts)
- Wide and rapid variations in input voltage levels
- Wide and rapid variations in input power frequency
- Electrical storms
- Large inductive sources (such as motors and welders)
- Faults in the distribution system wiring (such as loose connections)
- Microwave, radar, radio, or cell phone transmissions

Power System Protection

Computer systems can be protected from the sources of many of these electrical disturbances by using:

- A Protective Earth (PE) connection with a wire diameter of at least equal to the current carrying conductors. The neutral conductor must not be used for the PE connection. (The PE wire is GREEN with a YELLOW stripe.)
- A dedicated power distribution system
- Power conditioning equipment
- Over- and under-voltage detection and protection circuits
- Screening to cancel out the effects of undesirable transmissions
- Lightning arresters on power cables to protect equipment against electrical storms

Every precaution has been taken during power distribution system design to provide immunity to power outages of less than one cycle. However, testing cannot conclusively rule out loss of service. Therefore, adherence to the following guidelines provides the best possible performance of power distribution systems for Superdome server equipment:

- Dedicated power source—Isolates server power distribution system from other circuits in the facility.
- Missing-phase and low-voltage detectors—Shuts equipment down automatically when a severe power disruption occurs. For peripheral equipment, these devices are recommended but optional.
- Online uninterruptable power supply (UPS)—Keeps input voltage to devices constant and should be considered if outages of one-half cycle or more are common. Refer to qualified contractors or consultants for each situation.

1476 Paula

Distribution Hardware

This section describes wire selection and the types of raceways (electrical conduits) used in the distribution system. Wire size is dictated by circuit breaker sizing and local safety codes.

Wire Selection

Use copper conductors instead of aluminum, as aluminum's coefficient of expansion differs significantly from that of other metals used in power hardware. Because of this difference, aluminum conductors can cause connector hardware to work loose, overheat, and fail.

Raceway Systems (Electrical Conduits)

Raceways (electrical conduits) form part of the protective ground path for personnel and equipment. Raceways protect the wiring from accidental damage and also provide a heat sink for the wires.

Any of the following types may be used:

- Electrical metallic tubing (EMT) thin-wall tubing
- Rigid (metal) conduit
- Liquidtight with RFI strain relief (most commonly used with raised floors)
- Plenum-grade cables

Building Distribution

All building feeders and branch circuitry should be in rigid metallic conduit with proper connectors (to provide ground continuity). Conduit that is exposed and subject to damage should be constructed of rigid galvanized steel.

The IOX and Superdome are safety grounded through the green (ground) wire in each AC power cord. In the IOX, this ground passes through the AC power cord entry into the XPC and connects internally to the XPC chassis. The XUC chassis and each ICE chassis are grounded through their respective DC power cords from the XPC. Additional safety grounding must be provided for networking equipment.

Power Routing

Power drops and interface cables from the equipment are routed down from the power panel, through a grommet-protected opening (beneath the floor level), and under the floor panels.

Grounding Systems

Superdome servers require two methods of grounding:

- Power distribution safety grounding
- High frequency intercabinet grounding

Power Distribution Safety Grounding

The power distribution safety grounding system consists of connecting various points in the power distribution system to earth ground using green (green/yellow) wire ground conductors. Having these ground connections tied to metal chassis parts that may be touched protects computer room personnel against shock hazard from current leakage and fault conditions.

Power distribution systems consist of several parts. Hewlett-Packard recommends that these parts be solidly interconnected to provide an equipotential ground to all points.

NCR N 03/2005 - CN
CPMI - CORREIOS
1476
Fls:
Data: 3711

Main Building Electrical Ground The main electrical service entrance equipment should have an earth ground connection, as required by applicable codes. Connections such as a grounding rod, building steel, or a conductive type cold water service pipe provide an earth ground.

Electrical Conduit Ground To provide a continuous grounding system, all electrical conduits should be made of rigid metallic conduit that is securely connected together or bonded to panels and electrical boxes.

Power Panel Ground Each power panel should be grounded to the electrical service entrance with green (green/yellow) wire ground conductors. The green (green/yellow) wire ground conductors should be sized per applicable codes (based on circuit over current device ratings).

NOTE The green wire ground conductor mentioned above may be a black wire marked with green tape.

Computer Safety Ground Ground all computer equipment with the green (green/yellow) wire included in the branch circuitry. The green (green/yellow) wire ground conductors should be connected to the appropriate power panel and should be sized per applicable codes (based on circuit over current device ratings).

Superdome was approved by regulatory agencies around the world, and therefore requires a ground/protective earth. there are no exclusions to this regulatory approval.

High-frequency grounding between IOX and Superdome is provided by the cabinet-to-cabinet signal cabling. Whenever an IOX is connected to a Superdome cabinet, low-frequency grounding between these two cabinets is provided by a ground strap. This ground strap is shipped with each IOX. Refer to the *I/O Expansion Cabinet Guide* for more detail.

Newtwork-connected Equipment Ground The installation must provide a ground connection for the network equipment. This statement is translated into the following two languages as required:

WARNING **Sweden: Apparaten skall anslutas till jordat uttag, när den ansluts till ett nätverk.**

WARNING **Denmark: Før tilslutning af de øvrige ledere, se medfølgende installationsvejledning.**

System Installation Guidelines

This section contains information about installation practices. Some common pitfalls are highlighted. Both power cable and data communications cable installations are discussed.

Wiring Connections

Expansion and contraction rates vary among different metals. Therefore, the integrity of an electrical connection depends on the restraining force applied. Connections that are too tight compress or deform the hardware and causes it to weaken. This usually leads to high impedance causing circuit breakers to trip.

CAUTION Connections that are too loose have a high resistance that cause serious problems, such as erratic equipment operation. A high resistance connection overheats and sometimes causes fire or high temperatures that can destroy hard-to-replace components such as distribution panels or system bus bars.

E C
1474
PL - AC

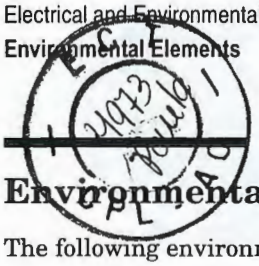
Wiring connections must be properly torqued. Many equipment manufacturers specify the proper connection torque values for their hardware.

Ground connections must only be made on a conductive, nonpainted surface. Lockwashers must be used on all connections to prevent connection hardware from working loose.

Data Communications Cables

Power transformers and heavy foot traffic create high energy fields. Route data communications cables away from these areas. Use shielded data communications cables that meet approved industry standards to reduce the effects of external fields. Data cables that are run externally to a metal fire enclosure must have a minimum fire rating of VW-1 or VW-4 or better.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1477
Fls:
3701
Doc: 43



Environmental Elements

The following environmental elements can affect a Superdome server installation:

- Computer room preparation
- Cooling requirements
- Humidity level
- Air conditioning ducts
- Dust and pollution control
- Electrostatic discharge (ESD) prevention
- Acoustics (noise reduction)
- Zinc whisker control

Computer Room Preparation

The following guidelines are recommended when preparing a computer room for a Superdome server system:

- Locate the computer room away from the exterior walls of the building to avoid the heat gain from windows and exterior wall surfaces.
- When exterior windows are unavoidable, use windows that are double- or triple-glazed and shaded to prevent direct sunlight from entering the computer room.
- Maintain the computer room at a positive pressure relative to surrounding spaces.
- Use a vapor barrier installed around the entire computer room envelope to restrain moisture migration.
- Caulk and vapor seal all pipes and cables that penetrate the envelope.
- Use at least a 12-inch raised floor system for the most favorable room air distribution system (underfloor distribution).
- Ensure a minimum ceiling height of 12 inches between the top of the server and the ceiling. Ensure all ceiling clips are in place.

Cooling Requirements

Air conditioning equipment requirements and recommendations are described in the following sections.

Basic Air Conditioning Equipment Requirements

The cooling capacity of the installed air conditioning equipment for the computer room should be sufficient to offset the computer equipment dissipation loads, as well as any space envelope heat gain. This equipment should include:

- Air filtration
- Cooling or dehumidification
- Humidification
- Reheating
- Air distribution

E&C
0972
Rubrica
DPL - AC

- System controls adequate to maintain the computer room within the operating ranges listed in Table 2-1.

Table 2-1 Computer Room Environment

Parameter	Operating Range	Recommended Range	Maximum Rate of Change (per hour)
Temperature[a,b]	68° to 86° F (20° to 30° C)	68 to 72 °F (20° to 23° C)	9° F repetitive, 36° F nonrepetitive (5° C repetitive, 20° C nonrepetitive)
Humidity	15% - 80% with no condensation (40% - 55% recommended)		6%

a. At altitudes up to 3,000 (9,842) meters.
b. System also requires 2400 CFM airflow.

Lighting and personnel must also be included. For example, a person dissipates about 450 BTUs per hour while performing a typical computer room task.

At altitudes above 10,000 feet (3048 m), the lower air density reduces the cooling capability of air conditioning systems. If your facility is located above this altitude, the recommended temperature ranges may need to be modified. For each 1000 feet (305 m) increase in altitude above 10,000 feet (up to a maximum of 15,000 feet), subtract 1.5° F (0.83° C) from the upper limit of the temperature range listed in Table 1-14 on page 31.

Air Conditioning System Guidelines

The following guidelines are recommended when designing an air conditioning system and selecting the necessary equipment:

- The air conditioning system serveing the computer room should be capable of operating 24 hours a day, 365 days a year. It should also be independent of other systems in the building.
- Consider the long-term value of computer system availability, redundant air conditioning equipment, or capacity.
- The system should be capable of handling any future computer system expansion.
- Air conditioning equipment air filters should have a minimum rating of 45% (based on "AShRA Standard 52-76, Dust Spot Efficiency Test").
- Introduce only enough outside air into the system to meet building code requirements (for human occupancy) and to maintain a positive air pressure in the computer room.

Air Conditioning System Types

The following three air conditioning system types are listed in order of preference:

- Complete self-contained package unit(s) with remote condenser(s). These systems are available with u, or down discharge and are usually located in the computer room.
- Chilled water package unit with remote chilled water plant. These systems are available with up or down discharge and are usually located in the computer room.
- Central station air handling units with remote refrigeration equipment. These systems are usually located outside the computer room.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1478
Fls:
Doc:

Basic Air Distribution Systems

A basic air distribution system includes supply air and return air.

An air distribution system should be zoned to deliver an adequate amount of supply air to the cooling air intake vents of the computer system equipment cabinets. Supply air temperature should be maintained within the following parameters:

- Ceiling supply system—From 55° F (12.8° C) to 60° F (15.6° C)
- Floor supply system—At least 60° F (15.6° C)

If a ceiling plenum return air system or a ducted ceiling return air system is used, the return air grille(s) in the ceiling should be located directly above the computer equipment cabinets.

The following three types of air distribution system are listed in order of recommendation:

- Underfloor air distribution system—Downflow air conditioning equipment located on the raised floor of the computer room uses the cavity beneath the raised floor as plenum for the supply air.

  Return air from an underfloor air distribution system can be ducted return air (DRA) above the ceiling, as shown in Figure 2-2 on page 48.

  Perforated floor panels (available from the raised floor manufacturer) should be located around the perimeter of the system cabinets. Supply air emitted though the perforated floor panels is then available near the cooling air intake vents of the computer system cabinets.

- Ceiling plenum air distribution system—Supply air is ducted into the ceiling plenum from upflow air conditioning equipment located in the computer room or from an air handling unit (remote).

  The ceiling construction should resist air leakage. Place perforated ceiling panels (with down discharge air flow characteristics) around the perimeter of the system cabinets. The supply air emitted downward from the perforated ceiling panels is then available near the cooling air intake vents of the computer system cabinets.

  Return air should be ducted back to the air conditioning equipment though the return air duct above the ceiling.

- Above ceiling ducted air distribution system—Supply air is ducted into a ceiling diffuser system from upflow air conditioning equipment located in the computer room or from an air handling unit (remote).

  Return air from an above ceiling ducted air distribution system may be ducted return air (DRA) above the ceiling, as shown in Figure 2-4 on page 50, or ceiling plenum return air (CPRA), as shown in Figure 2-3 on page 49.

  Adjust the supply air diffuser system grilles to direct the cooling air downward around the perimeter of the computer system cabinets. The supply air is then available near the cooling air intake vents of the computer system cabinets.

Air Conditioning System Installation

All air conditioning equipment, materials, and installation must comply with any applicable construction codes. Installation of the various components of the air conditioning system must also conform to the air conditioning equipment manufacturer's recommendations.

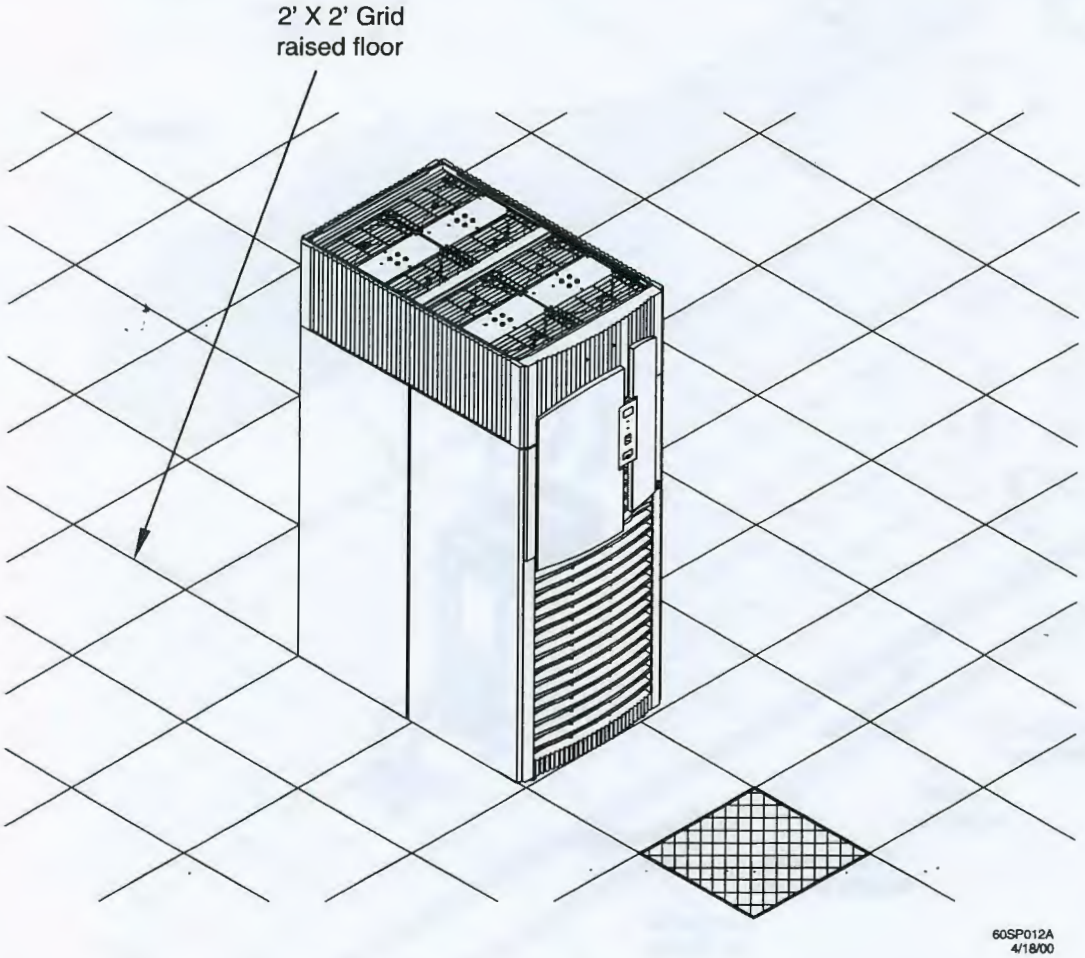
Figure 2-2 on page 48 illustrates a typical computer room underfloor air distribution system (DRA).

Figure 2-3 on page 49 illustrates a typical computer room ceiling plenum air distribution system (CPRA).

E C T
S 4470
L - A

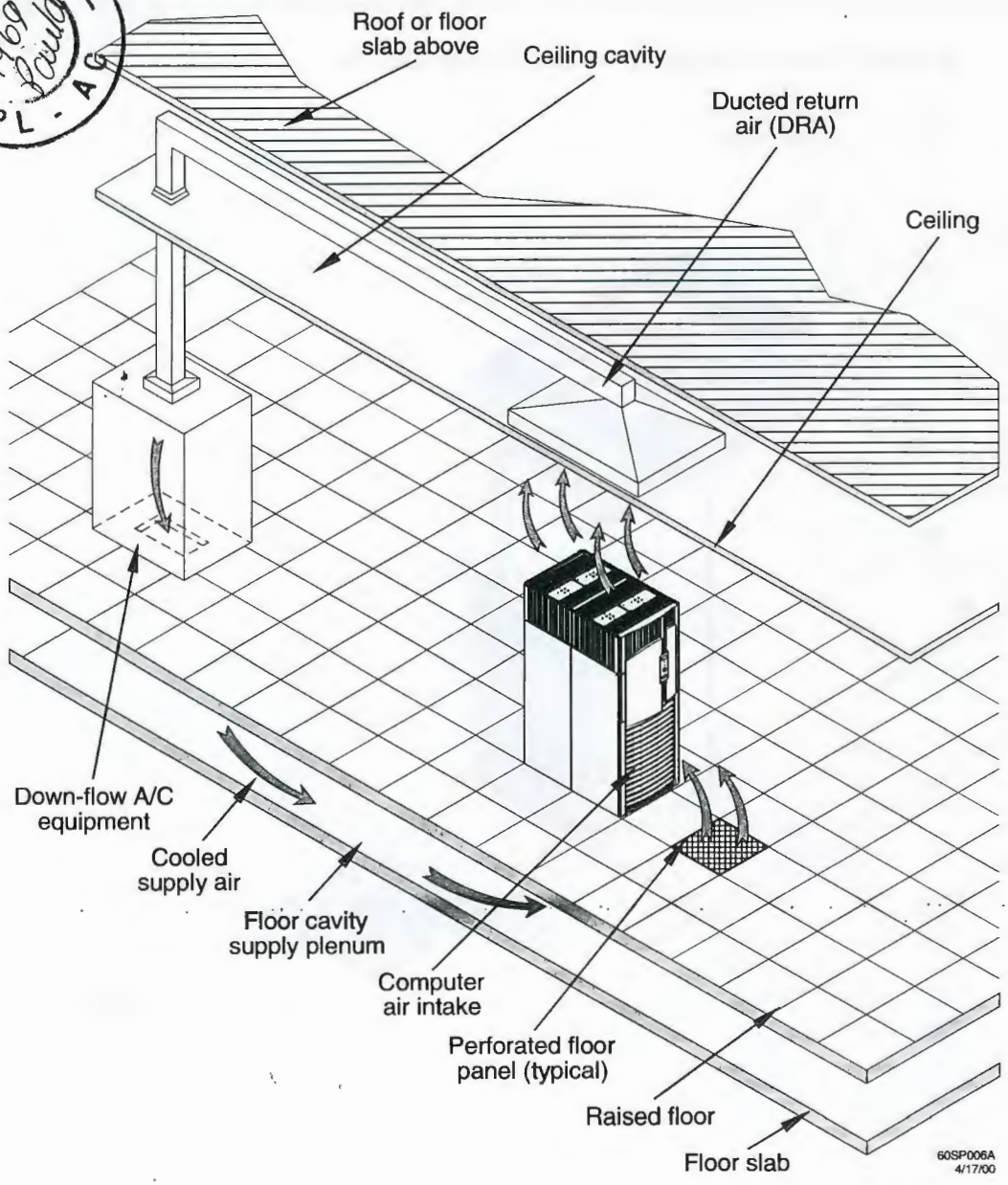
Figure 2-4 on page 50 illustrates a typical computer room above ceiling ducted air distribution system (DRA).

Figure 2-1 Typical Computer Room Raised Floor Layout



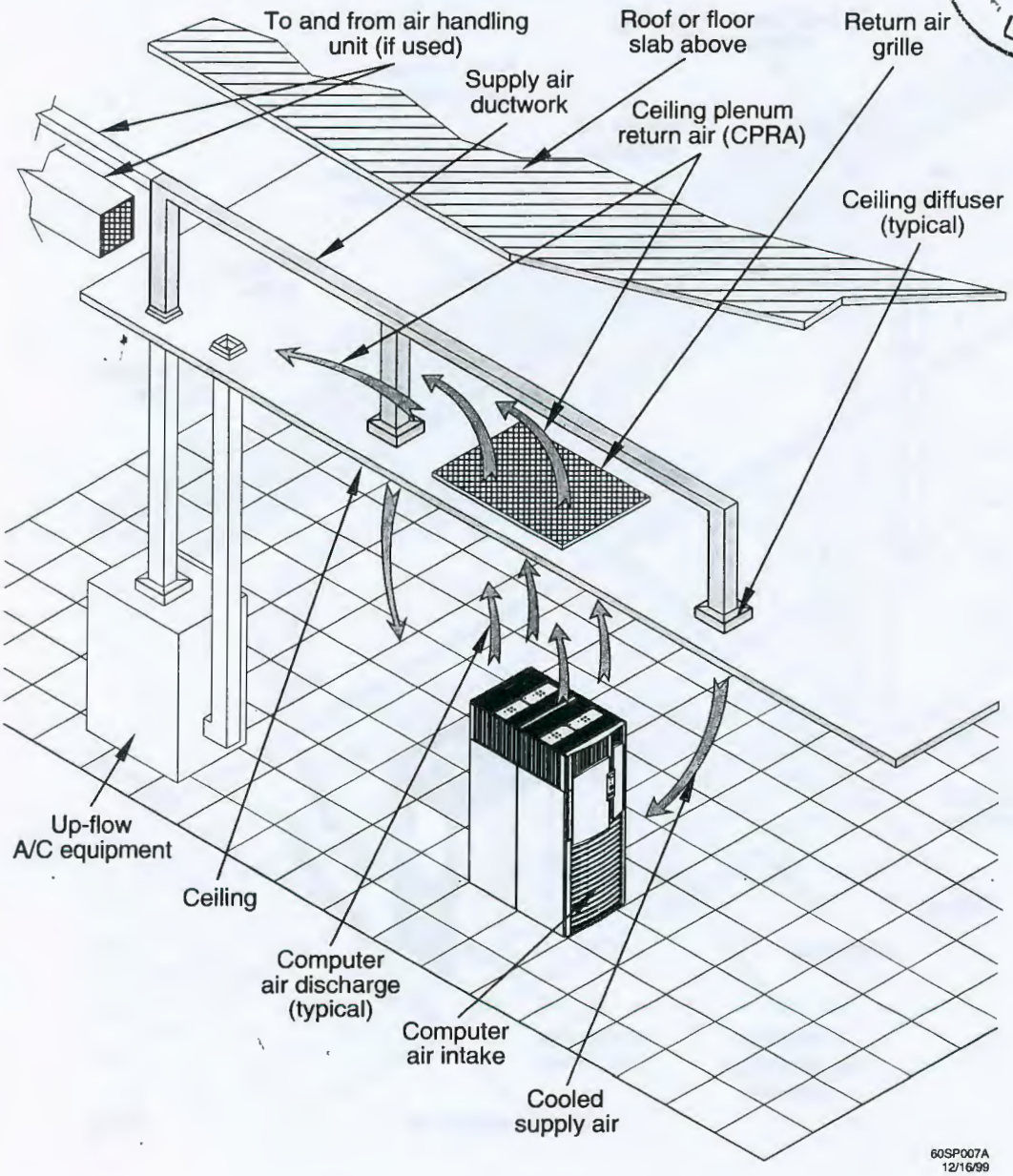
RQS Nº 03/2005 - CN
CPMI - CORREIOS
1479
Fls: 3701
Doc: 47

Figure 2-2 Underfloor Air Distribution System



ECT 4968 Paula 1 L - AC

Figure 2-3 Ceiling Plenum Air Distribution System



RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1480
3701
Doc:

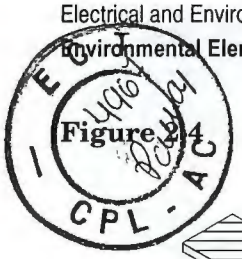
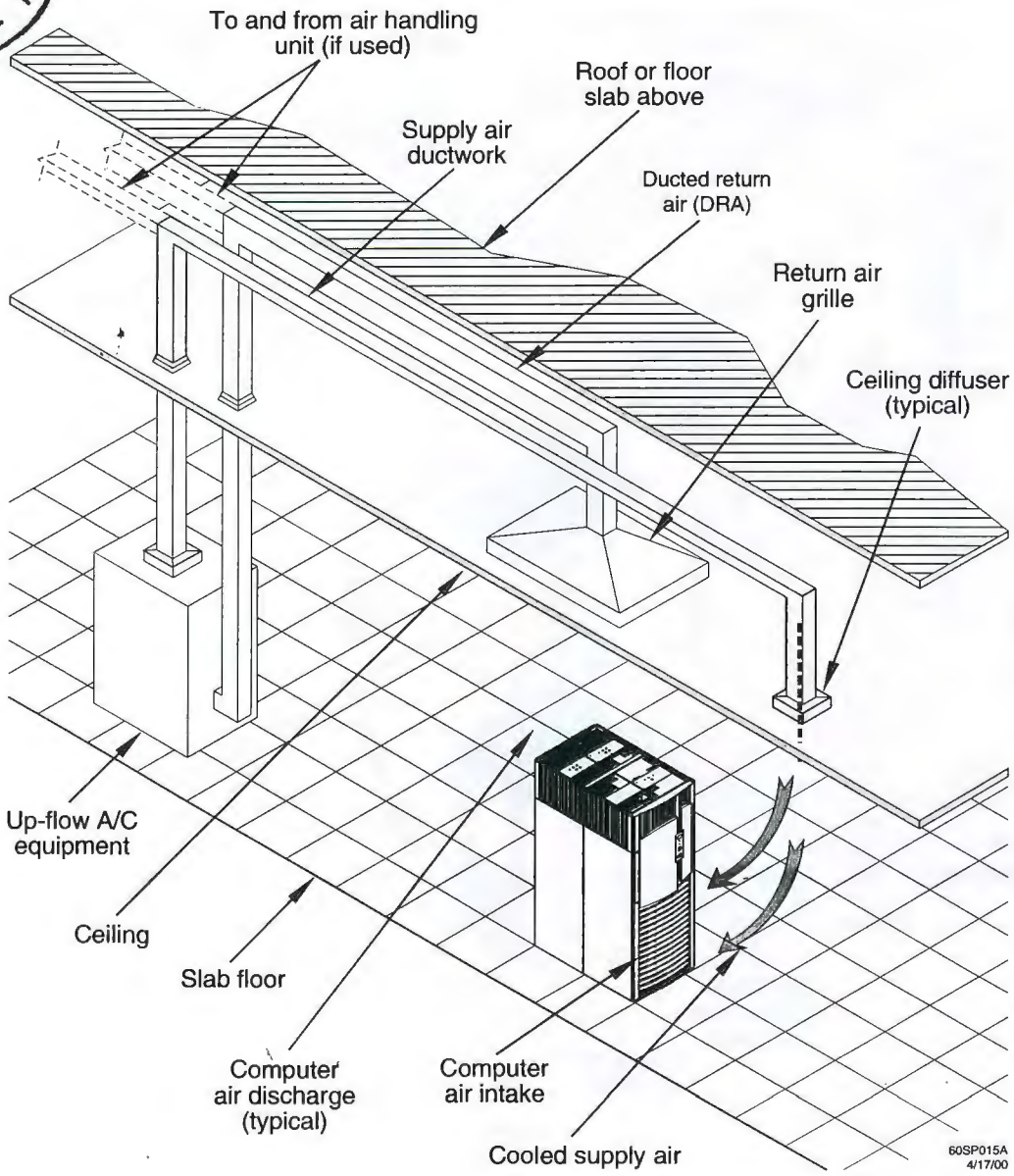


Figure 2-4 Above Ceiling Ducted Air



Humidity Level

Maintain proper humidity levels. High humidity causes galvanic actions to occur between some dissimilar metals. This eventually causes a high resistance between connections, leading to equipment failures. High humidity can also have an adverse affect on some magnetic tapes and paper media.

E C T 4966 Fls: 1 Rubrica CPL - AC

CAUTION Low humidity contributes to undesirably high levels of electrostatic charges. This increases the electrostatic discharge (ESD) voltage potential. ESD can cause component damage during servicing operations. Paper feed problems on high-speed printers are usually encountered in low-humidity environments.

Low humidity levels are often the result of the facility heating system and occur during the cold season. Most heating systems cause air to have a low humidity level, unless the system has a built-in humidifier.

Air Conditioning Ducts

Use separate computer room air conditioning duct work. If it is not separate from the rest of the building, it might be difficult to control cooling and air pressure levels. Duct work seals are important for maintaining a balanced air conditioning system and high static air pressure. Adequate cooling capacity means little if the direction and rate of air flow cannot be controlled because of poor duct sealing. Also, the ducts should not be exposed to warm air, or humidity levels may increase.

Dust and Pollution Control

Computer equipment can be adversely affected by dust and microscopic particles in the site environment.

Specifically, disk drives, tape drives, and some other mechanical devices can have bearing failures resulting from airborne abrasive particles. Dust may also blanket electronic components like printed circuit boards causing premature failure due to excess heat and/or humidity build up on the boards. Other failures to power supplies and other electronic components can be caused by metallically conductive particles. These metallic particles are conductive and can short circuit electronic components. Use every effort to ensure that the environment is as dust and particulant free as possible.

Smaller particles can pass though some filters and, over a period of time, possibly cause problems in mechanical parts. Small dust particles can be prevented from entering the computer room by maintaining its air conditioning system at a high static air pressure level.

Other sources of dust, metallic, conductive, abrasive, and/or microscopic particles can be present. Some sources of these particulants are:

- Subfloor shedding
- Raised floor shedding
- Ceiling tile shedding

These pollutants are not always visible to the naked eye. A good check to determine their possible presence is to check the underside of the tiles. The tile should be shiny, galvanized, and free from rust.

The computer room should be kept clean. The following guidelines are recommended:

- Smoking—Establish a no-smoking policy. Cigarette smoke particles are eight times larger than the clearance between disk drive read/write heads and the disk surface.
- Printer—Locate printers and paper products in a separate room to eliminate paper particulate problems.
- Eating or drinking—Establish a no-eating or drinking policy. Spilled liquids can cause short circuits in equipment such as keyboards.
- Tile floors—Use a dust-absorbent cloth mop rather than a dry mop to clean tile floors.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1481
Doc: 3701

Special precautions are necessary if the computer room is near a source of air pollution. Some air pollutants, especially hydrogen sulfide (H2S), are not only unpleasant but corrosive as well. Hydrogen sulfide damages wiring and delicate sound equipment. The use of activated charcoal filters reduces this form of air pollution.

Zinc Particulate Contamination

Metallic particulates can be especially harmful around electronic equipment. This type of contamination may enter the data center environment from a variety of sources, including but not limited to raised floor tiles, worn air conditioning parts, heating ducts, rotor brushes in vacuum cleaners or printer component wear. Because metallic particulates conduct electricity, they have an increased potential for creating short circuits in electronic equipment. This problem is exaggerated by the increasingly dense circuitry of electronic equipment.

Over time, very fine whiskers of pure metal can form on electroplated zinc, cadmium, or tin surfaces. If these whiskers are disturbed, they may break off and become airborne, possibly causing failures or operational interruptions. For over 50 years, the electronics industry has been aware of the relatively rare but possible threat posed by metallic particulate contamination. During recent years, a growing concern has developed in computer rooms where these conductive contaminants are formed on the bottom of some raised floor tiles.

Although this problem is relatively rare, it may be an issue within your computer room. Since metallic contamination can cause permanent or intermittent failures on your electronic equipment, Hewlett-Packard strongly recommends that your site be evaluated for metallic particulate contamination before installation of electronic equipment.

Electrostatic Discharge (ESD) Prevention

Static charges (voltage levels) occur when objects are separated or rubbed together. The voltage level of a static charge is determined by the following factors:

- Types of materials
- Relative humidity
- Rate of change or separation

Table 2-2 lists charge levels based on personnel activities and humidity levels.

Table 2-2 Effect of Humidity on ESD Charge Levels

Personnel Activity[a]	Humidity[b] and Charge Levels (volts)[c]			
	26%	32%	40%	50%
Walking across a linoleum floor	6,150	5,750	4,625	3,700
Walking across a carpeted floor	18,450	17,250	13,875	11,100
Getting up from a plastic chair	24,600	23,000	18,500	14,800

a. Source: B.A.Unger, Electrostatic Discharge Failures of Semiconductor Devices (Bell Laboratories,1981)
b. For the same relative humidity level, a high rate of airflow produces higher static charges than a low airflow rate.
c. Some data in this table has been extrapolated.

E C T
4964
Paulo
CPL - AC

Static Protection Measures

Follow these precautions to minimize possible ESD-induced failures in the computer room:

- Install conductive flooring (conductive adhesive must be used when laying tiles).
- Use conductive wax (if waxed floors are necessary).
- Ensure that all equipment and flooring are properly grounded and are at the same ground potential.
- Use conductive tables and chairs.
- Use a grounded wrist strap (or other grounding method) when handling circuit boards.
- Store spare electronic modules in antistatic containers.
- Maintain recommended humidity level and airflow rates in the computer room.

Acoustics

Computer equipment and air conditioning blowers cause computer rooms to be noisy. Ambient noise level in a computer room can be reduced as follows:

- Dropped ceiling—Cover with a commercial grade of fire-resistant, acoustic rated, fiberglass ceiling tile.
- Sound deadening—Cover the walls with curtains or other sound deadening material.
- Removable partitions—Use foam rubber models for most effectiveness.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1482
Doc: 3758

E C T
4965
Paula
CPL - AC

3 Facility Guidelines

This chapter describes facility characteristics and provides guidelines for preparing the computer room.

- "Facility Characteristics" on page 57 discusses architectural issues.
- "Space Requirements" on page 60 discusses the amount of floor space required by the components.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1483
Fls:
3701
Doc:

NOTE

Refer to Appendix C for templates to aid in locating caster contact area and caster/leveling foot centers. Templates are also provided to locate required cutouts for cable routing.

Facility Characteristics

This section contains information about facility characteristics that must be considered for the installation or operation of a Superdome server. Facility characteristics are:

- Floor loading
- Windows
- Altitude effects

Floor Loading

The computer room floor must be able to support the total weight of the installed computer system as well as the weight of the individual cabinets as they are moved into position.

Floor loading is usually not an issue in non-raised-floor installations. The information presented in this section is directed toward raised-floor installations.

NOTE Any floor system under consideration for a Superdome server installation should be verified by an appropriate floor system consultant.

Raised-Floor Loading

Raised-floor loading is a function of the manufacturer's load specification and the positioning of the equipment relative to the raised-floor grid. While Hewlett-Packard cannot assume responsibility for determining the suitability of a particular raised-floor system, information and illustrations are provided for the customer or local agencies to determine installation requirements.

The following guidelines are recommended:

- Because many raised-floor systems do not have grid stringers between floor stands, the lateral support for the floor stands depends on adjacent panels being in place. To avoid compromising this type of floor system while gaining under floor access, remove only one floor panel at a time.
- Larger floor grids (bigger panels) are generally rated for lighter loads.

CAUTION Do not install any raised-floor system until you have carefully examined it to verify that it is adequate to support the appropriate installation.

Floor-Loading Terms

Table 3-1 defines floor-loading terms.

Table 3-1 Floor-Loading Terms

Term	Definition
Dead load	Weight of the raised-panel floor system, including the understructure. Expressed in lb/ft2 (kg/m2).
Live load	Load the floor system can safely support. Expressed in lb/ft2 (kg/m2).

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1484
Fls:
3701
Doc:

Table 3-1 Floor-Loading Terms (Continued)

Term	Definition
Concentrated load	Load a floor panel can support on a 1-in2 (6.45 cm2) area at the panel's weakest point (typically the center of the panel), without the surface of the panel deflecting more than a predetermined amount.
Ultimate load	Maximum load (per floor panel) the floor system can support without failure. Failure expressed by floor panel(s) breaking or bending. Ultimate load is usually stated as load per floor panel.
Rolling load	Load a floor panel can support (without failure) when a wheel of specified diameter and width is rolled across the panel.
Average floor load	Computed by dividing total equipment weight by the area of its footprint. This value is expressed in lb/ft2 (kg/m2).

Average Floor Loading

The average floor load value, defined in Table 3-2, is not appropriate for addressing raised-floor ratings at the floor grid spacing level. However, it is useful for determining floor-loading at the building level, such as the area of solid floor or span of raised-floor tiles covered by the Superdome server footprint.

Typical Raised-Floor Site

This section contains an example of a computer room raised-floor system that is satisfactory for the installation of a Superdome server.

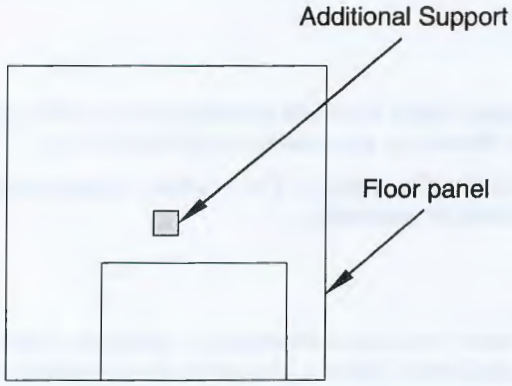
Based on specific information provided by Hewlett-Packard, Tate Access Floors has approved its Series 800 all-steel access floor with bolt-together stringers and 24 in. (61.0 cm) by 24 in. (61.0 cm) floor panels.

Due to the large amount of floor panel material that must be removed for the purpose of routing cables, this particular floor must be braced as shown in Figure 3-1.

E C T
Facility Guidelines
Facility Characteristics
AC

In the event that the flooring is being replaced or a new floor is being installed, Tate Access Floors recommends its Series 1250 all-steel access floor with bolt-together stringers and 24 in. (61.0 cm) by 24 in. (61.0 cm) floor panels be used to support the Superdome installation.

Figure 3-1 Tate Series 800 Floor Bracing



NOTE If the specific floor being evaluated or considered is other than a Tate Series 800 floor, the specific floor manufacturer must be contacted to evaluate the floor being used.

Table 3-2 lists specifications for the Tate Access Floors Series 800 raised-floor system.

Table 3-2 Tate Series 800 Raised-Floor Tile Specifications

Item	Rating
Dead load	7 lb/ft 2 (34.2 kg/m2)
Live load	313 lb/ft 2 (1528.3 kg/m2)
Concentrated load[a]	1250 lb (567 kg)
Ultimate load	4000 lb (1814 kg) per panel
Rolling load	400 lb (181 kg)
Average Tile load	500 lb (227 kg)

a. With 0.08 in (0.2 cm) of span maximum deflection

Windows

Avoid housing computers in a room with windows. Sunlight entering a computer room may cause problems. Magnetic tape storage media is damaged if exposed to direct sunlight. Also, the heat generated by sunlight places an additional load on the cooling system.

POS N° 03/2005 - GN
CPMI CORREIOS
1485
Fls:
Doc: 3701

Space Requirements

This section contains information about space requirements for a Superdome server. This data should be used as the basic guideline for space plan developments. Other factors, such as airflow, lighting, and equipment space requirements, must also be considered.

Delivery Space Requirements

There should be enough clearance to move equipment safely from the receiving area to the computer room. Permanent obstructions, such as pillars or narrow doorways, can cause equipment damage.

Delivery plans should include the possible removal of walls or doors. The physical dimensions for applicable computers and peripheral equipment are summarized in Appendix A.

Operational Space Requirements

Other factors must be considered along with the basic equipment dimensions. Reduced airflow around equipment causes overheating, which can lead to equipment failure. Therefore, the location and orientation of air conditioning ducts, as well as airflow direction, are important. Obstructions to equipment intake or exhaust airflow must be eliminated.

The location of lighting fixtures and utility outlets affects servicing operations. Plan equipment layout to take advantage of lighting and utility outlets. Do not forget to include clearance for opening and closing equipment doors.

Clearance around and above the cabinets must be provided for proper cooling airflow through the equipment.

The service area space requirements, outlined in Appendix C, are minimum dimensions. If other equipment is located so that it exhausts heated air near the cooling air intakes of the computer system cabinets, larger space requirements are needed to keep ambient air intake to the computer system cabinets within the specified temperature and humidity ranges.

Space planning should also include the possible addition of equipment or other changes in space requirements. Equipment layout plans should also include provisions for the following:

- Channels or fixtures used for routing data cables and power cables
- Access to air conditioning ducts, filters, lighting, and electrical power hardware
- Power conditioning equipment
- Cabinets for cleaning materials
- Maintenance area and spare parts

Floor Plan Grid

The floor plan grid is used to plan the location of equipment in the computer room. In addition to its use for planning, the floor plan grid should also be used when planning the locations of the following items:

- Air conditioning vents
- Lighting fixtures
- Utility outlets
- Doors

Facility Guidelines
Space Requirements

- Access areas for power wiring and air conditioning filters
- Equipment cable routing

Copies of the floor plan grid are located in Appendix C.

Equipment Footprint Templates

Equipment footprint templates are provided in Appendix C to show basic equipment dimensions and space requirements for servicing. Be sure to use the appropriate templates for the equipment that is to be installed.

The service areas shown on the template drawings are lightly shaded.

Removable copies of the equipment footprint templates are located in Appendix C. They should be used with the floor plan grid to define the location of the equipment that will be installed in your computer room.

NOTE Photocopying typically changes the scale of drawings copied. If any templates are copied, then all templates and floor plan grids must also be copied.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1486
Fls: 370
Doc:

FCT
CPL - AC
2458
Paula

E C T
24957 Paula
CPL - AC I

4 Pre-Installation Survey

This chapter provides a site survey information packet consisting of an information form and checklists to be used to evaluate a computer facility. The checklists information sheets and information forms should be filled out by the customer and a Hewlett-Packard representative.

- "Pre-Installation Survey Content" on page 65 describes the contents of the site survey information packet.

ECT 2005 - CN
CPMI - CORREIOS
Fls: 1487
Doc: 3791

"Typical Installation Schedule" on page 66 describes the proposed schedule of installation events.

"Site Inspection" on page 67 provides a sample pf the on-site inspection checklist.

"Delivery Survey" on page 71 provides the delivery or installation requirement forms.

ECT 4955 Paula AC 1

Pre-Installation Survey Content

The site pre-installation survey information is designed to identify problems that might occur before, during, or after the installation of the system. It contains the following items:

- Pre-installation checklists—Verify the customer site is ready for the equipment installation.
- Pre-installation survey information sheets—List customer name, address, and corresponding Hewlett-Packard sales personnel.
- Pre-installation survey information forms—List delivery information and special instructions.

ROS Nº 03/2005 - CN
CPMI - CORREIOS
1488
Fls:
Doc: 65 7 01

Typical Installation Schedule

The following schedule lists the sequence of events for a typical system installation:

- 60 days before installation
  - — Floor plan design completed and mailed to Hewlett-Packard
- 30 days before installation
  - — Primary power and air conditioning installation completed
  - — Telephone and data cables installed
  - — Fire protection equipment installed
  - — Major facility changes completed
  - — Special delivery requirements defined
  - — Site inspection survey completed
  - — Delivery survey completed
  - — Signed copy of the site inspection and delivery survey mailed to Hewlett-Packard
  - — Site inspection and pre-delivery coordination meeting arranged with a Hewlett-Packard representative to review the inspection checklist and arrange an installation schedule.
- 7 days before installation
  - — Final check made with a Hewlett-Packard customer engineer to resolve any last-minute problems

Pre-Installation Survey
Site Inspection

Site Inspection

Table 4-1 contains a sample of the Customer and Hewlett-Packard information required.

Table 4-2 contains a sample site inspection checklist.

IMPORTANT Ensure that the customer is aware of the iCOD email requirements. That is, each bootable partition requires a connection to the internet to send email to notify Hewlett-Packard that the customer has allocated additional CPUs beyond the amount initially purchased. Each bootable partition must be configured to perform this operation.

For more details, go to http://superdome.hp.com and click on the iCOD link.

NOTE Table 4-1 and Table 4-2 are provided as examples only. To ensure use of the current information specific to your site preparation, refer to the Site Readiness Review Section of the Deployment Manager's Handbook.

Table 4-1 Customer and Hewlett-Packard Information

Customer Information	
Name:	Phone No:
Street Address:	City or Town:
State or Province:	Country
Zip or postal code:	
Primary customer contact:	Phone No.:
Secondary customer contact:	Phone No.:
Traffic coordinator:	Phone No.:
Hewlett-Packard information	
Sales representative	Order No:
Representative making survey	Date:
Scheduled delivery date	

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1489
Fls:
3771
67
Doc:

NOTE To ensure compliance with item 10 of Table 4-2, provide a copy of Appendix D to the customer to use a worksheet to identify required names and addresses for the LAN.

Table 4-2 Site Inspection Checklist

Please check either Yes or No. If No, include comment or date				Comment or Date
Computer room				
No.	Area or condition	Yes	No	
1.	Is there a completed floor plan?			
2.	Is there adequate space for maintenance needs? Front 42 in (106 cm) min., 48 in (121 cm) recommended. Rear 32 in (81 cm) min., 36 in (91cm) recommended			
3.	Is access to the site or computer room restricted?			
4.	Is the computer room structurally complete? Expected date of completion?			
5.	Is a raised floor installed and in good condition? What is the floor to ceiling height? [7.5 ft (228 cm) minimum]			
6.	Is the raised floor adequate for equipment loading?			
7.	Are there channels or cutouts for cable routing?			
8.	Is there a remote console telephone line available with an RJ11 jack?			
9.	Is a telephone line available?			
9a.	Is the customer aware of the iCOD email requirements? Each bootable partition requires a connection to the internet to send email to notify Hewlett-Packard that the customer has allocated additional CPUs beyond the amount initially purchased. Each bootable partition must be configured to perform this operation. For more details, go to http://superdome.hp.com and click on the iCOD link.			
10.	Are customer supplied peripheral and LAN cables available and of the proper type?			

Pre-Installation Survey
Site Inspection

Table 4-2 Site Inspection Checklist (Continued)

Please check either Yes or No. If No, include comment or date				Comment or Date
11.	Are floor tiles in good condition and properly braced?			
12.	Metallic particulate test required.			
Power and lighting				
No.	Area or condition	Yes	No	
13.	Are lighting levels adequate for maintenance?			
14.	Are there ac outlets available for servicing needs? (i.e. vacuuming)			
15.	Does the input voltage correspond to equipment specifications?			
15A	Is dual source power used? If so, identify type(s) and evaluate grounding.			
16	Does the input frequency correspond to equipment specifications?			
17.	Are lightning arrestors installed inside the building?			
18.	Is power conditioning equipment installed?			
19.	Is there a dedicated branch circuit for equipment?			
20.	Is the dedicated branch circuit less than 250 feet (72.5 meters)?			
21.	Are the input circuit breakers adequate for equipment loads?			
Safety				
No.	Area or condition	Yes	No	
22.	Is there an emergency power shut-off switch?			
23.	Is there a telephone available for emergency purposes?			
24.	Is there a fire protection system in the computer room?			
25.	Is antistatic flooring installed?			

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1490
Fls:
69
3701
Doc:

Table 4-2 Site Inspection Checklist (Continued)

Please check either Yes or No. If No, include comment or date				Comment or Date
26.	Are there any equipment servicing hazards (loose ground wires, poor lighting, etc.)?			
Cooling				
No.	Area or condition	Yes	No	
27.	Can cooling be maintained between 68° and 86° (20° and 30° C)?			
28.	Can temperature changes be held to 9° (5 ° C) per hour?			
29.	Can humidity level be maintained between 40% and 55%?			
30.	Are air conditioning filters installed and clean?			
Storage				
No.	Area or condition	Yes	No	
31.	Are cabinets available for tape and disc media?			
32.	Is shelving available for documentation?			
Training				
No.	Area or Condition			
33	Are personnel enrolled in the System Administrator's Course?			
34	Is on-site training required?			

E. C. T.
4949
Paula
CPL - AC

Delivery Survey

The delivery survey form shown in Figure 4-1 on page 72 and Figure 4-2 on page 73 lists delivery or installation requirements. If any of the items on the list apply, enter the appropriate information in the areas provided on the form.

Special instructions or recommendations should be entered on the Special Instructions or Recommendations form. Following are examples of special instructions or issues:

- Packaging restrictions at the facility, such as size and weight limitations
- Special delivery procedures
- Special equipment required for installation, such as tracking or hoists
- What time the facility is available for installation (after the equipment is unloaded)
- Special security requirements applicable to the facility, such as security clearance

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1491
Fls: 71
Doc: 3701

Figure 4-1 Delivery Survey (Part 1)

DELIVERY CHECKLIST

DOCK DELIVERY

Is dock large enough for a semitrailer? Yes _____ No _____

Circle the location of the dock and give street name if different than address.

North

West East

South

STREET DELIVERY

Circle the location of access door and list street name if different than address.

North

West East

South

List height _____ and width _____ of access door.

List special permits (if required) for street delivery.

Permit type: Agency obtained from:

_____ _____

_____ _____

60SP018A
12/7/99

Pre-Installation Survey
Delivery Survey
4947
CPL - AC

Figure 4-2 Delivery Survey (Part 2)

ELEVATOR

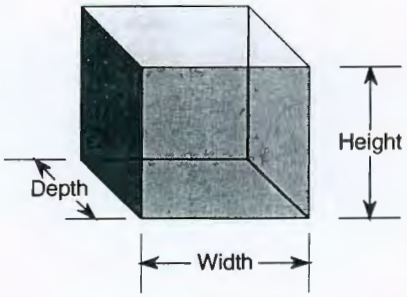
Fill in the following information if an elevator is required to move equipment.

Capacity (lb or kg) _____

Depth _____

Height _____

Width _____



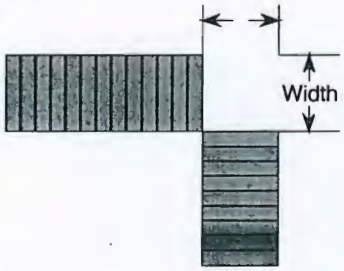
STAIRS

Please list number of flights and stairway dimensions.

Number of flights _____

Width _____

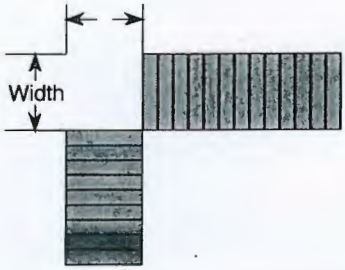
Width _____



Number of flights _____

Width _____

Width _____



60SP019A
11/24/99

RQS Nº 03/2005 - CN
CPMI - CORREIOS
73
1492
Fls: 3701
Doc:

E C T
4945
Paula
A C

A System Weights

RQS Nº 03/2005 - CN
CPMI - CORREIOS
75
1493
Fls:
Doc: 3701

Weight

To determine overall weight, follow the examples in Table A-1, then complete the entries in Table A-2.

Table A-1 Example Weight Summary

Component	Quantity	Multiply By	Weight (kg)
Chassis[a]	1	745.17 lbs (338.10)	745.17 lbs (338.10)
Cell Boards	4	41.00 lbs (18.60)	164.00 lbs (74.40)
DIMMs	128	.2 lbs (.09)	25.60 (11.60)
I/O Cardcages	4	36.5 lbs (16.56)	146 lbs (66.24)
I/O Cards	12	.45 lbs (.225)	5.4 lbs (2.45)
PDCA	2	26.00lbs (23.59)	104.00 lbs (47.18)
Bulk Power Supply (BPS)	6	23.00 lbs (11.81)	138.00 lbs (62.64)
		Total weight	1328.17lbs (517.35)

a. The listed weight for a chassis includes the weight of all components not listed in Table A-1.

Table A-2 Weight Summary

Component	Quantity	Multiply By	Weight (kg)
Chassis[a]		745.17 lbs (338.10)	745.17 lbs (338.10)
Cell Boards		41.00 lbs (18.60)	lbs
DIMMs		.2 lbs (.09)	lbs
I/O Cardcages		36.5 lbs (16.56)	lbs
I/O Cards		.45 lbs (.225)	lbs

E C T
4943
Paula
A C

Table A-2 Weight Summary (Continued)

Component	Quantity	Multiply By	Weight (kg)
PDCA		26.00lbs (23.59)	lbs
Bulk Power Supply (BPS)		23.00 lbs (11.81)	lbs
		Total weight	lbs

a. The listed weight for a chassis includes the weight of all components not listed in Table A-2.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1494
Doc: 3701

E C T
São Paulo
C P L - A C

B Conversion Factors

The conversion factors provided in this appendix are intended to ease data calculation for systems that do not conform specifically to the configurations listed in this Site Preparation Guide.

Listed below are the conversion factors used in this document, as well as additional conversion factors that may be helpful in determining those factors required for site planning.

ROS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1495
Doc: 3701

Refrigeration

- 1 watt = .86 kcal/h
- 1 watt = 3.413 Btu/h
- 1 watt = 2.843-4 tons
- 1 ton = 200 Btu/min
- 1 ton = 12,000 Btu/h
- 1 ton = 3,517.2 W

- Metric equivalents
  - 1 centimeter = 0.3937 in
  - 1 meter = 3.28 ft
  - 1 meter = 1.09 yds
  - 1 in. = 2.54 cm
  - 1 ft = 0.305 m
  - 1 CFM = 1.7m3/h
- kVA conversions, three ø

  $kVA = V \times A \times \sqrt{3} / 1000$
- kVA conversion, single ø

  $kVA = V \times A / 1000$

E C T
4939
Paula
L - AC

C Templates

This appendix contains blank floor plan grids and equipment templates. Combine the necessary number of floor plan grid sheets to create a scaled version of the computer room floor plan.

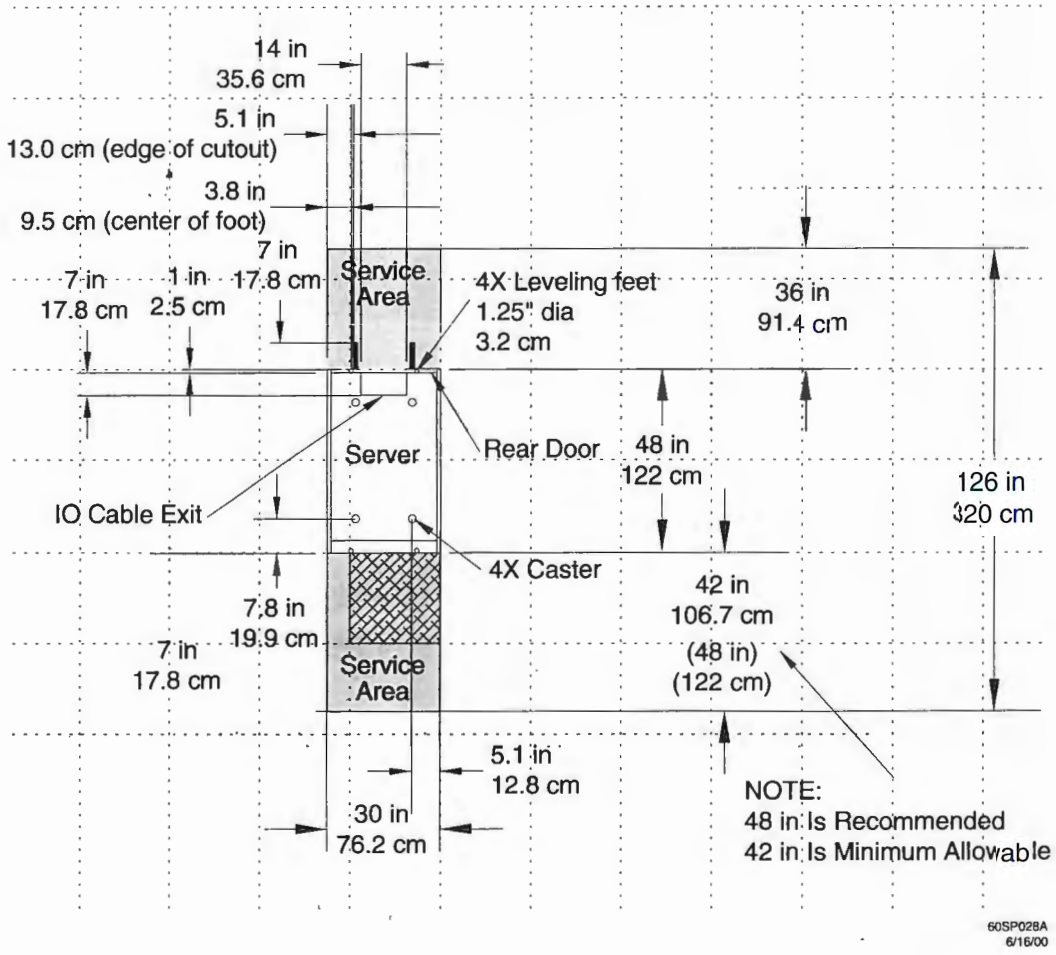
Figure C-1 illustrates the locations required for the cable cutouts.

Figure C-2 on page 83 illustrates the overall dimensions required for a Superdome 32 Way system.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1496
3701
Doc:

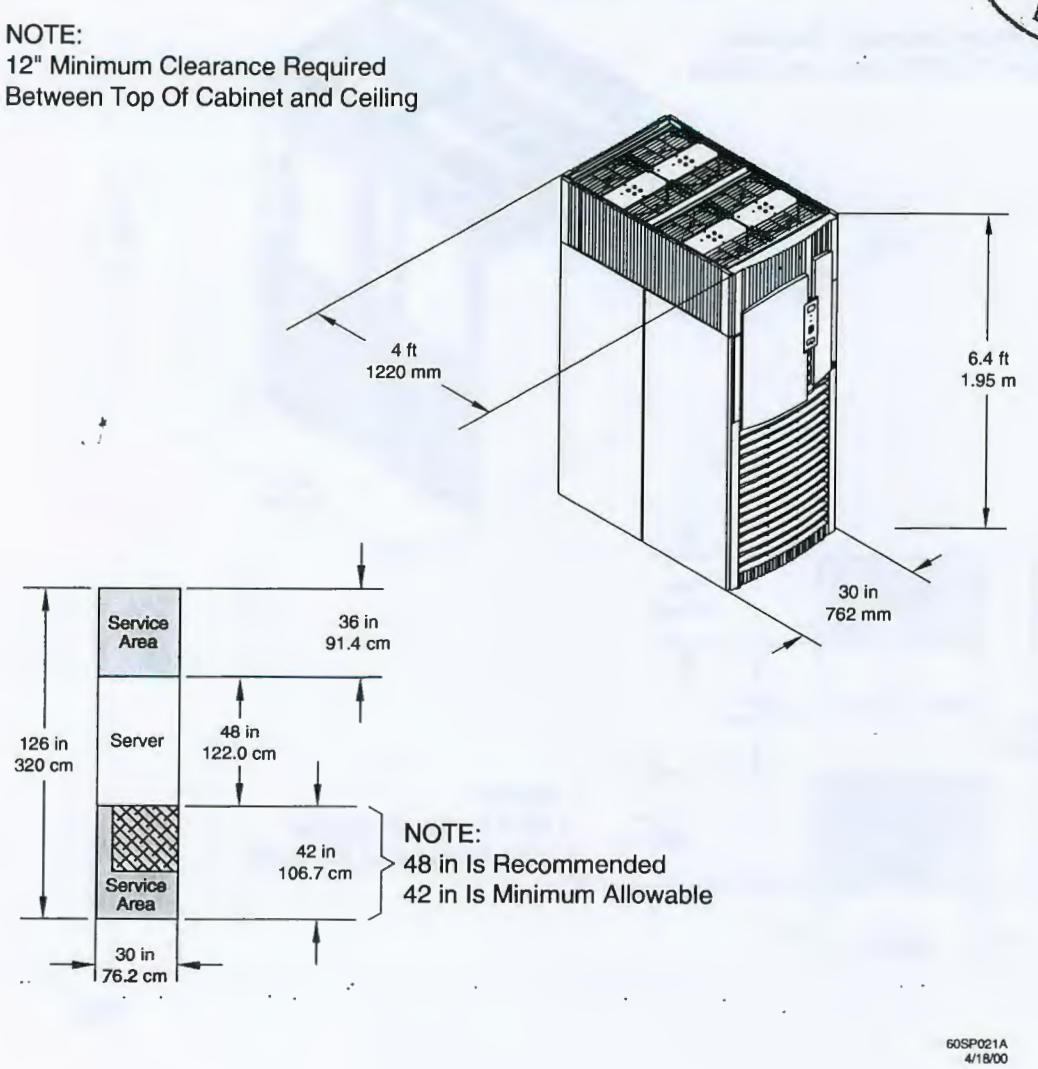
Figure C-3 on page 84 illustrates the overall dimensions required for a Superdome 64 Way system.

Figure C-1 Cable Cutouts and Caster Locations



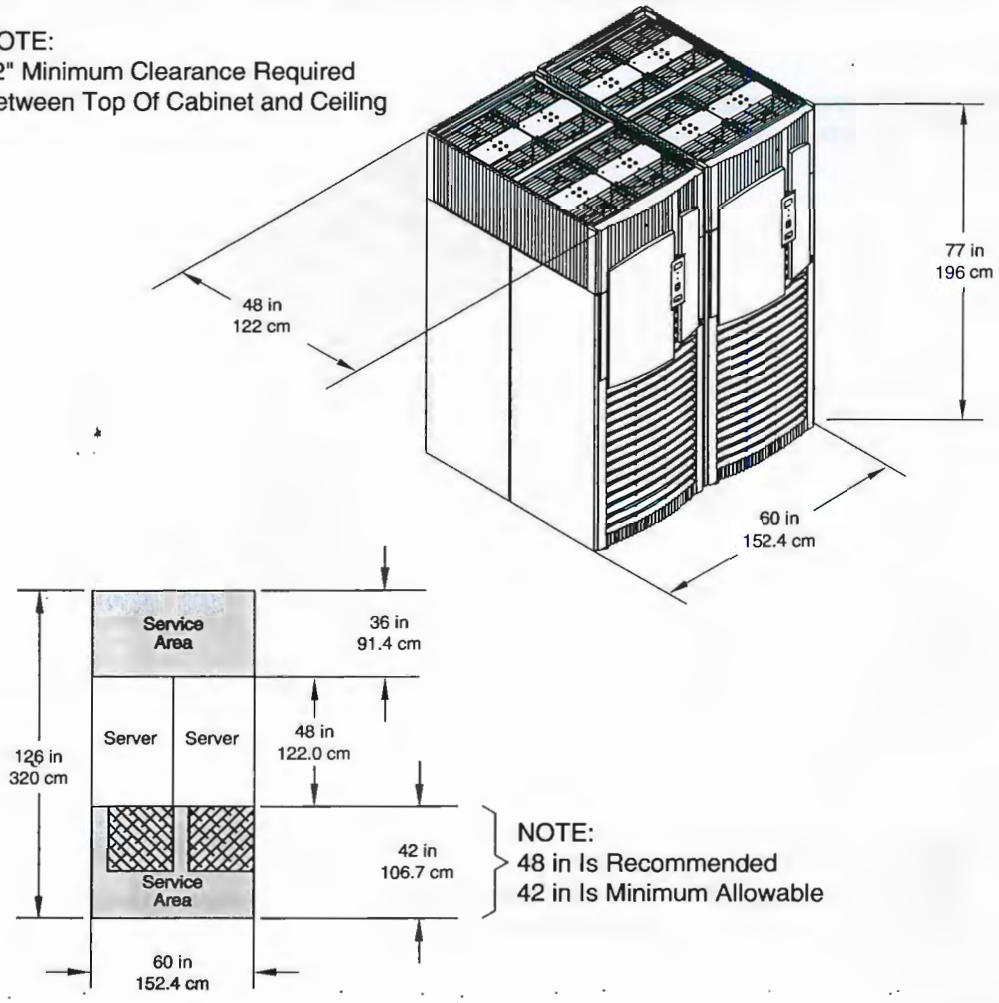
Templates
4937 Paula
CPL - AC

Figure C-2 Superdome 16 Way/Superdome 32 Way Space Requirements



RQS Nº 03/2005 - CN
CPMI - CORREIOS
1497
Fls:
3701
Doc:

Figure C-3 Superdome 64 Way Space Requirements



E C T
4935
Paula
A C

Equipment Footprint Templates

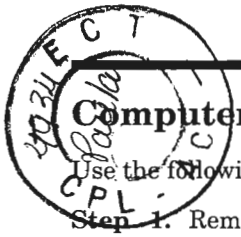
Equipment footprint templates are drawn to the same scale as the floor plan grid (1/4 inch = 1 foot). These templates are provided to show basic equipment dimensions and space requirements for servicing.

The service areas shown on the template drawings are lightly shaded.

The equipment templates should be used with the floor plan grid to define the location of the equipment that will be installed in your computer room.

NOTE Photocopying typically changes the scale of copied drawings. If any templates are copied, then all templates and floor plan grids must also be copied.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1498
Doc: 3701



Computer Room Layout Plan

Use the following procedure to create a computer room layout plan:

Step 1. Remove several copies of the floor plan grid.

Step 2. Cut and join them together (as necessary) to create a scale model floor plan of your computer room.

Step 3. Remove a copy of each applicable equipment footprint template.

Step 4. Cut out each template selected in Step 3; then place it on the floor plan grid created in Step 2.

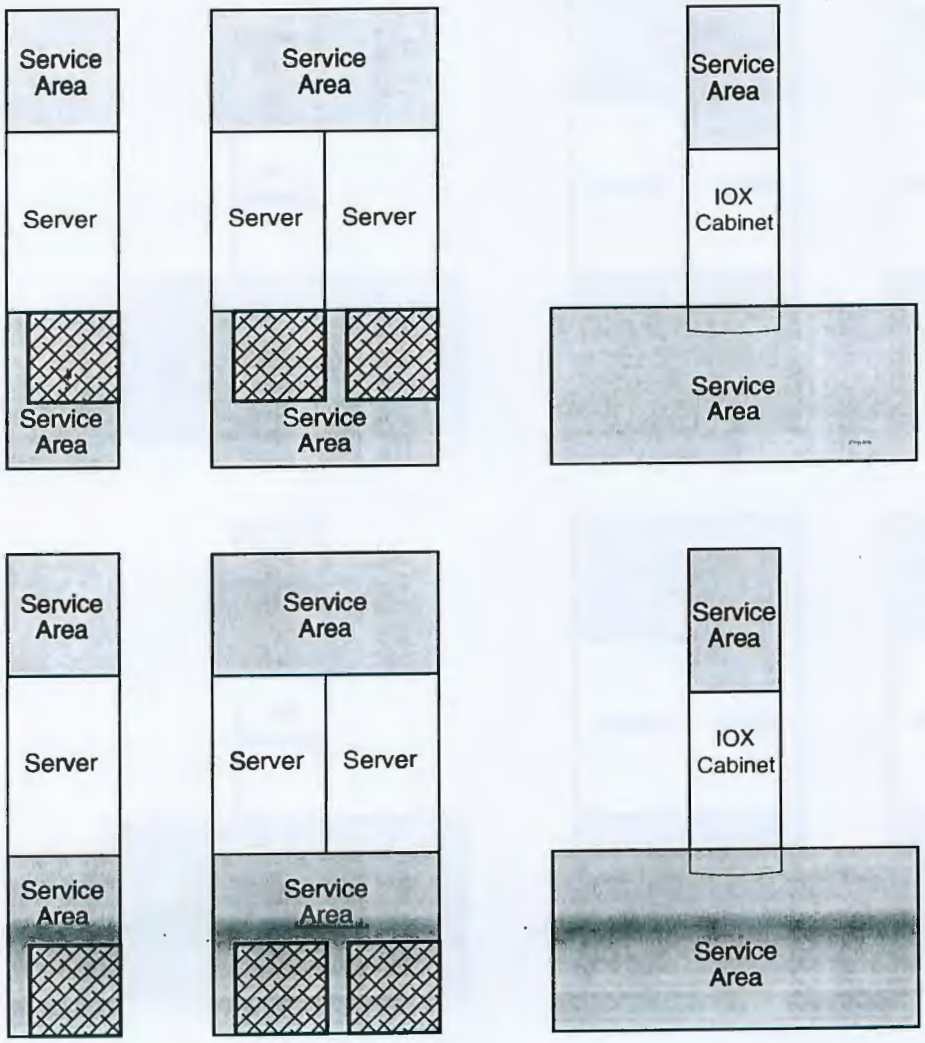
Step 5. Position pieces until the desired layout is obtained; then fasten the pieces to the grid. Mark locations of computer room doors, air-conditioning floor vents, utility outlets, and so on.

NOTE Attach a reduced copy of the completed floor plan to the site survey located in Chapter 4, "Pre-installation Survey." Hewlett-Packard field engineers use this floor plan during equipment installation.

4933
Paula
AC

Superdome 32 Way, Superdome 64 Way, and I/O Expansion Cabinet Templates

Scale: 1/4 inch = 1 foot

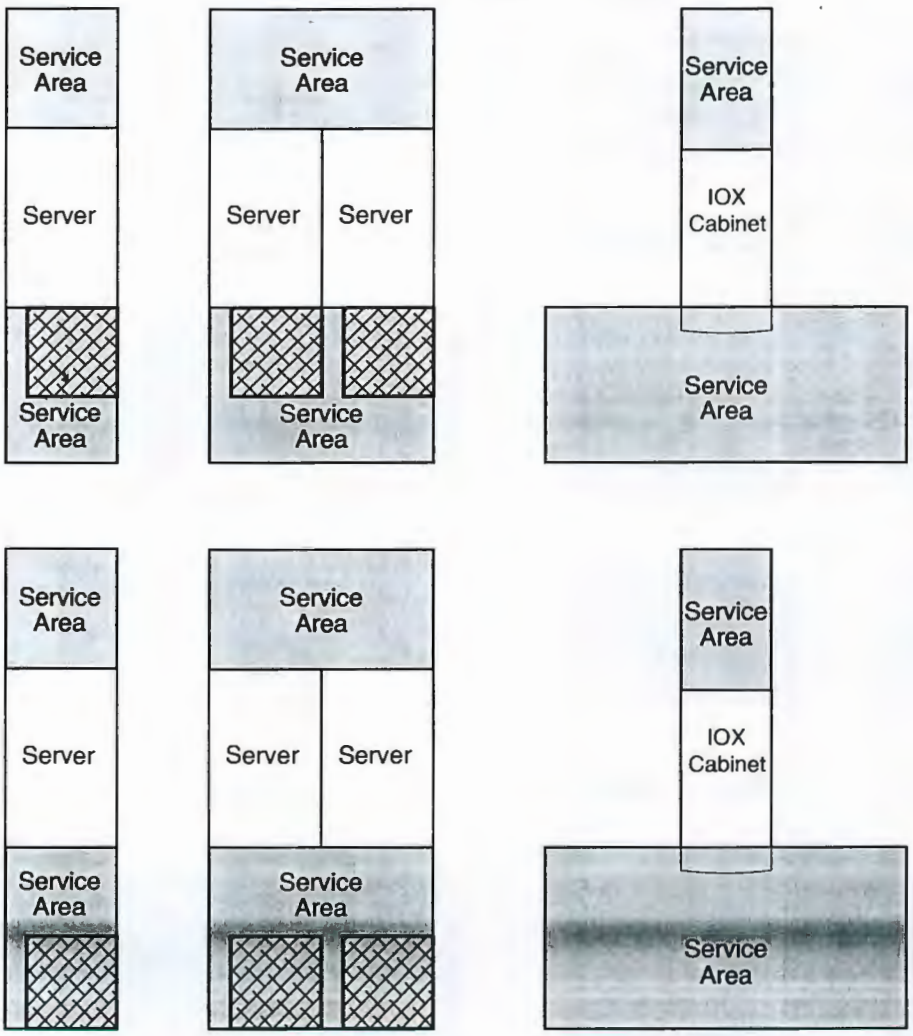


60SP017A
7/16/00

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1499
3701
Doc:

Superdome 32 Way, Superdome 64 Way, and I/O Expansion Cabinet Templates

Scale: 1/4 inch = 1 foot

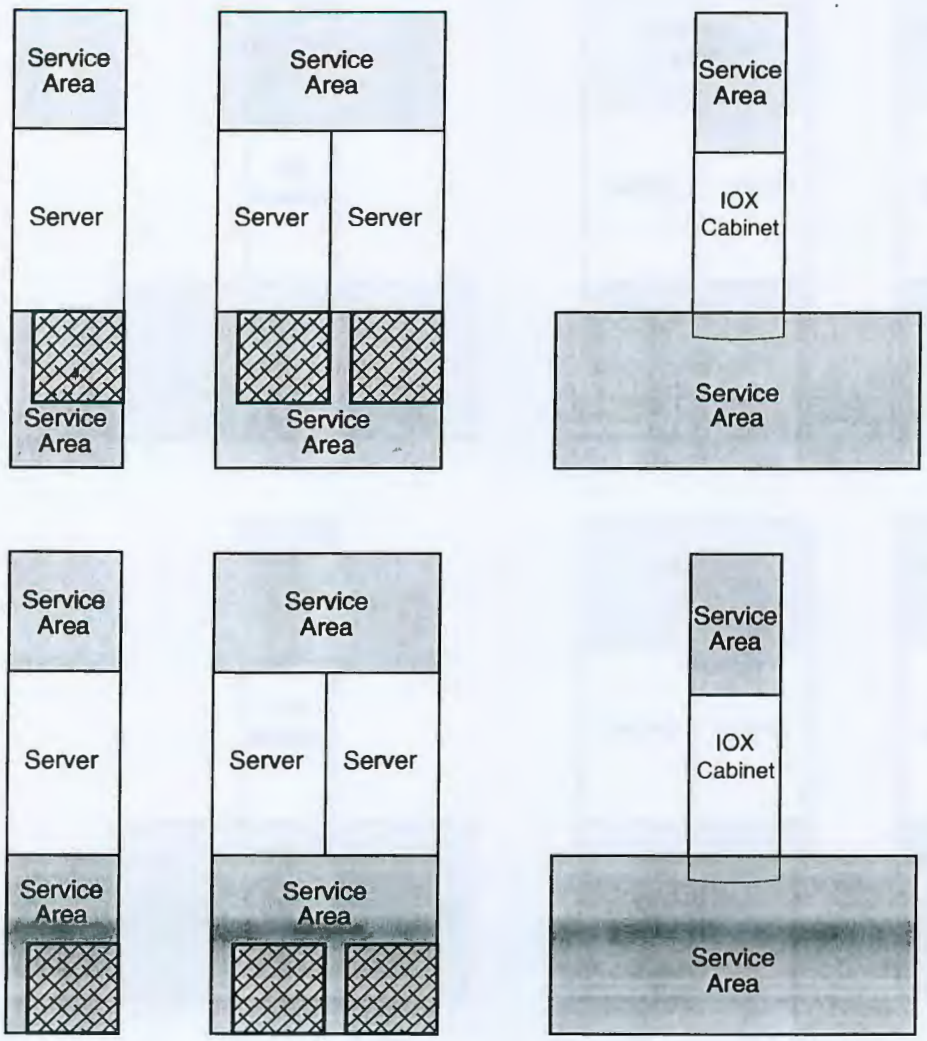


60SP017A
7/16/00

E Templates
Computer Room Layout Plan
4931
Paula
CPL - AC

Superdome 32 Way, Superdome 64 Way, and I/O Expansion Cabinet Templates

Scale: 1/4 inch = 1 foot

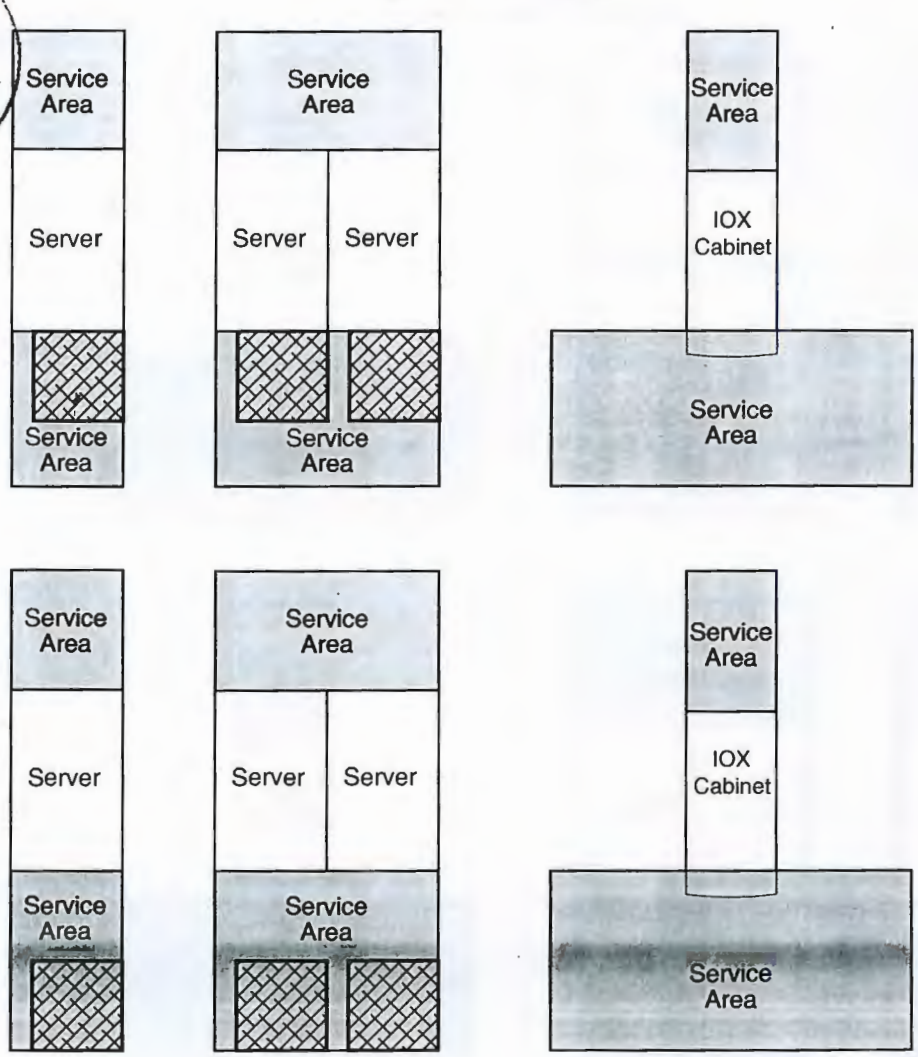


60SP017A
7/16/00

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1500
3701
Doc:

Superdome 32 Way, Superdome 64 Way, and I/O Expansion Cabinet Templates

Scale: 1/4 inch = 1 foot

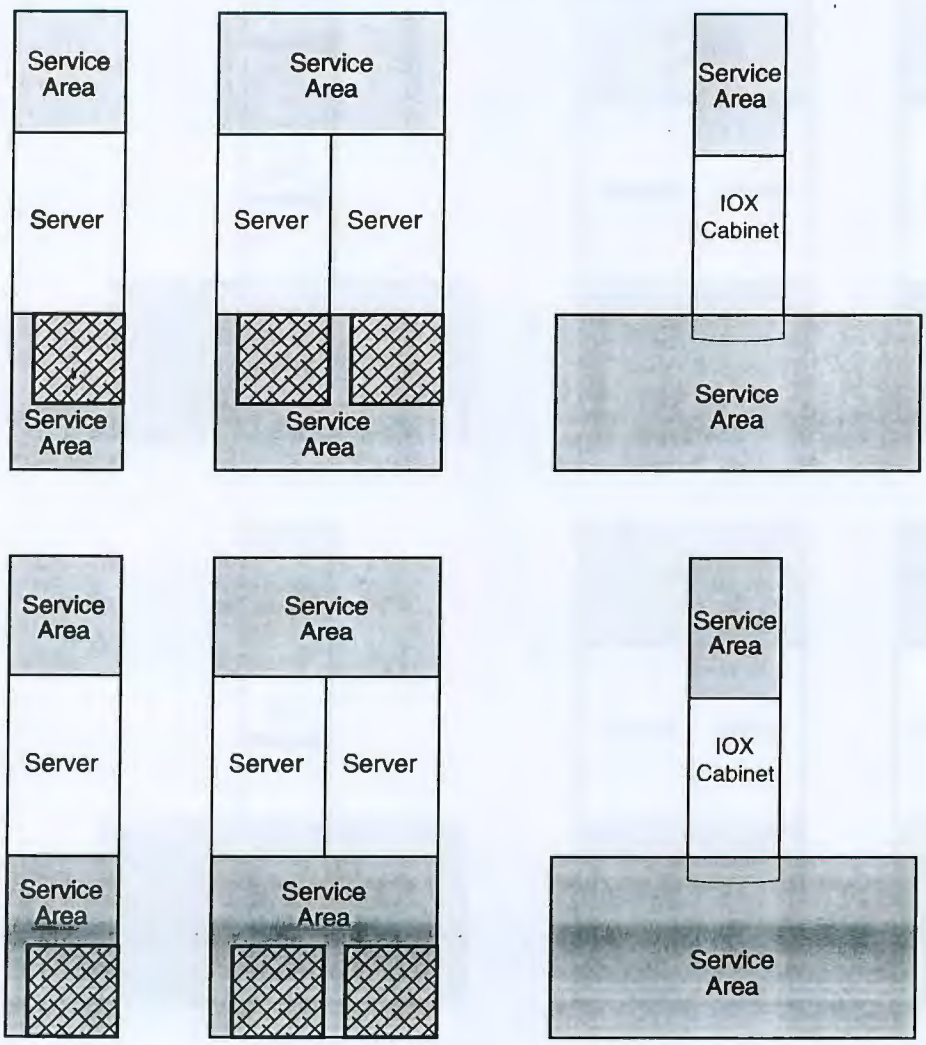


60SP017A
7/16/00

Templates
Computer Room Layout Plan

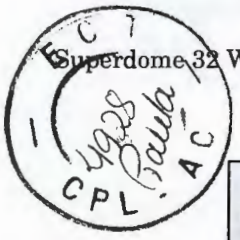
Superdome 32 Way, Superdome 64 Way, and I/O Expansion Cabinet Templates

Scale: 1/4 inch = 1 foot



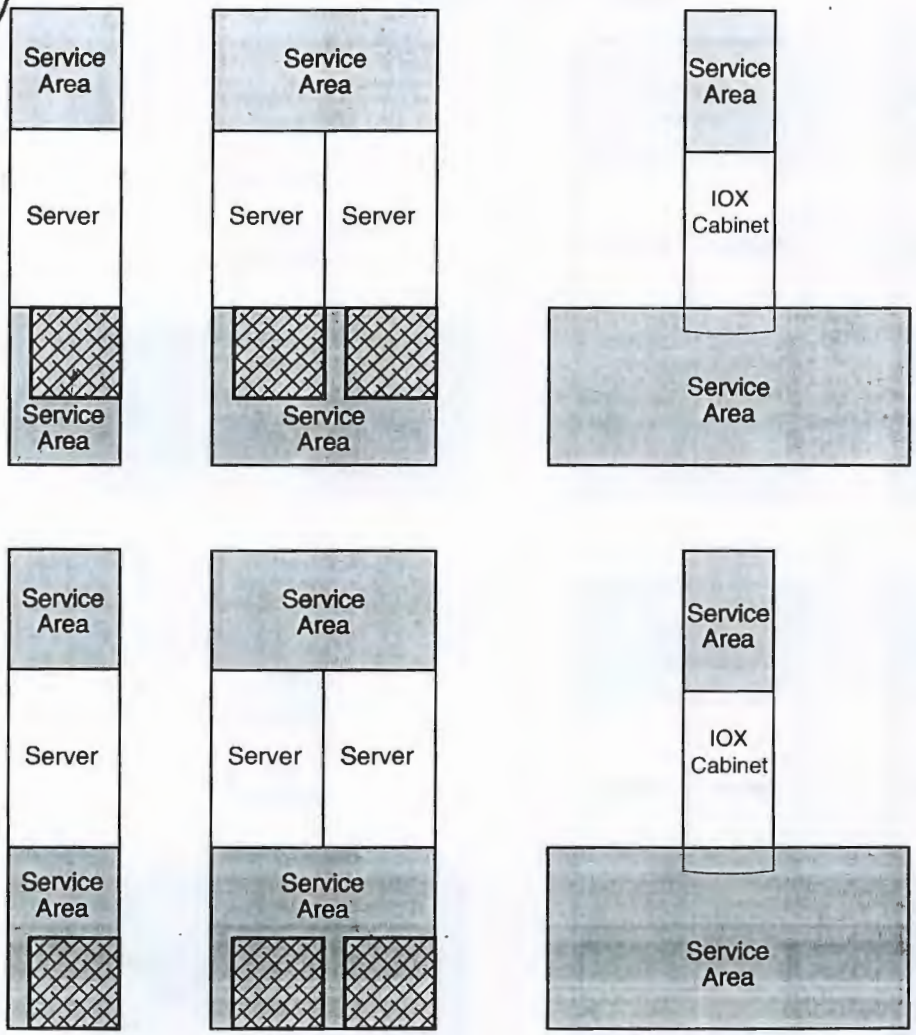
60SP017A
7/16/00

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1501
Doc: 3701



Superdome 32 Way, Superdome 64 Way, and I/O Expansion Cabinet Templates

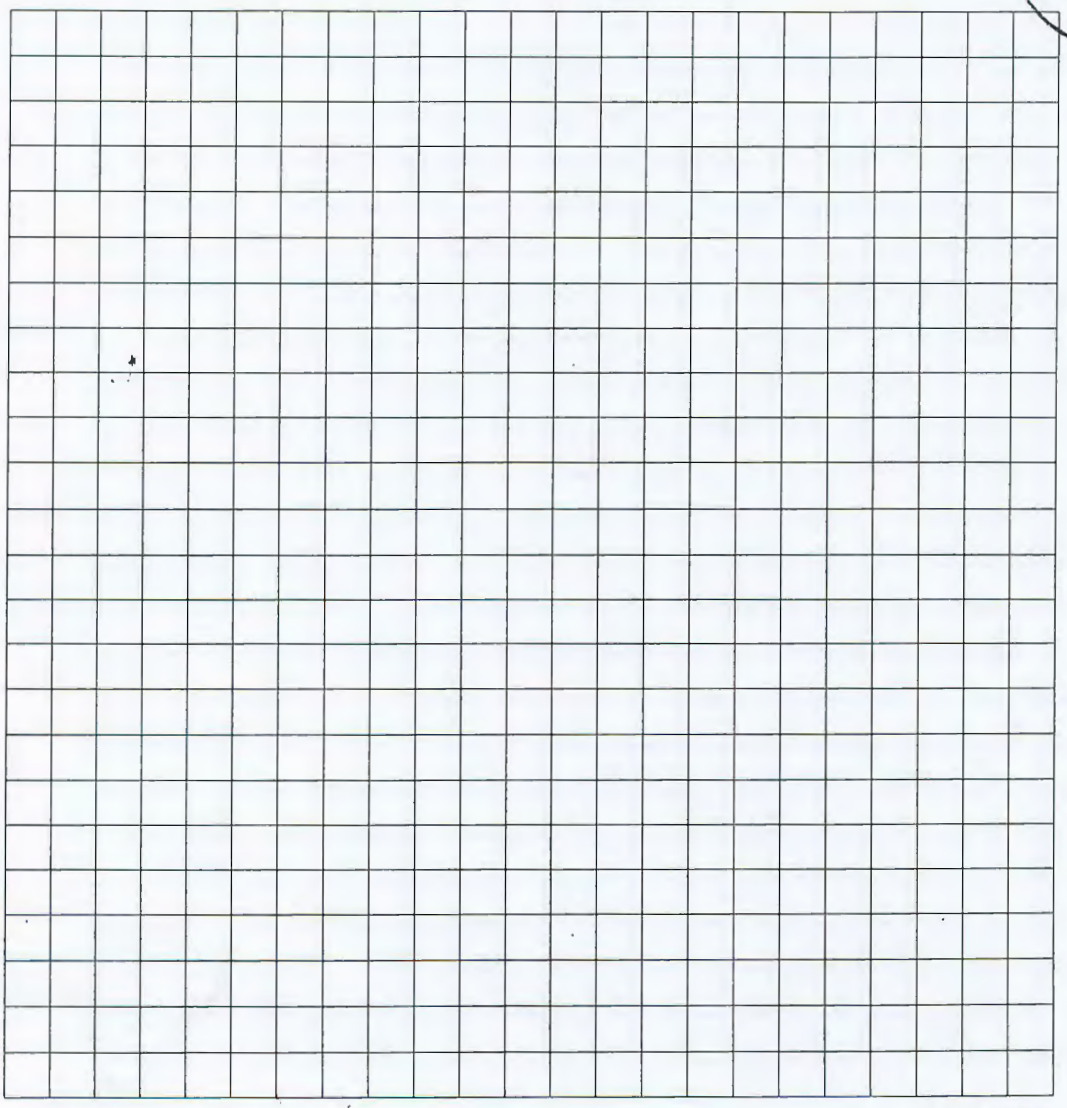
Scale: 1/4 inch = 1 foot



60SP017A
7/16/00

E C T
1927
Paula
A C

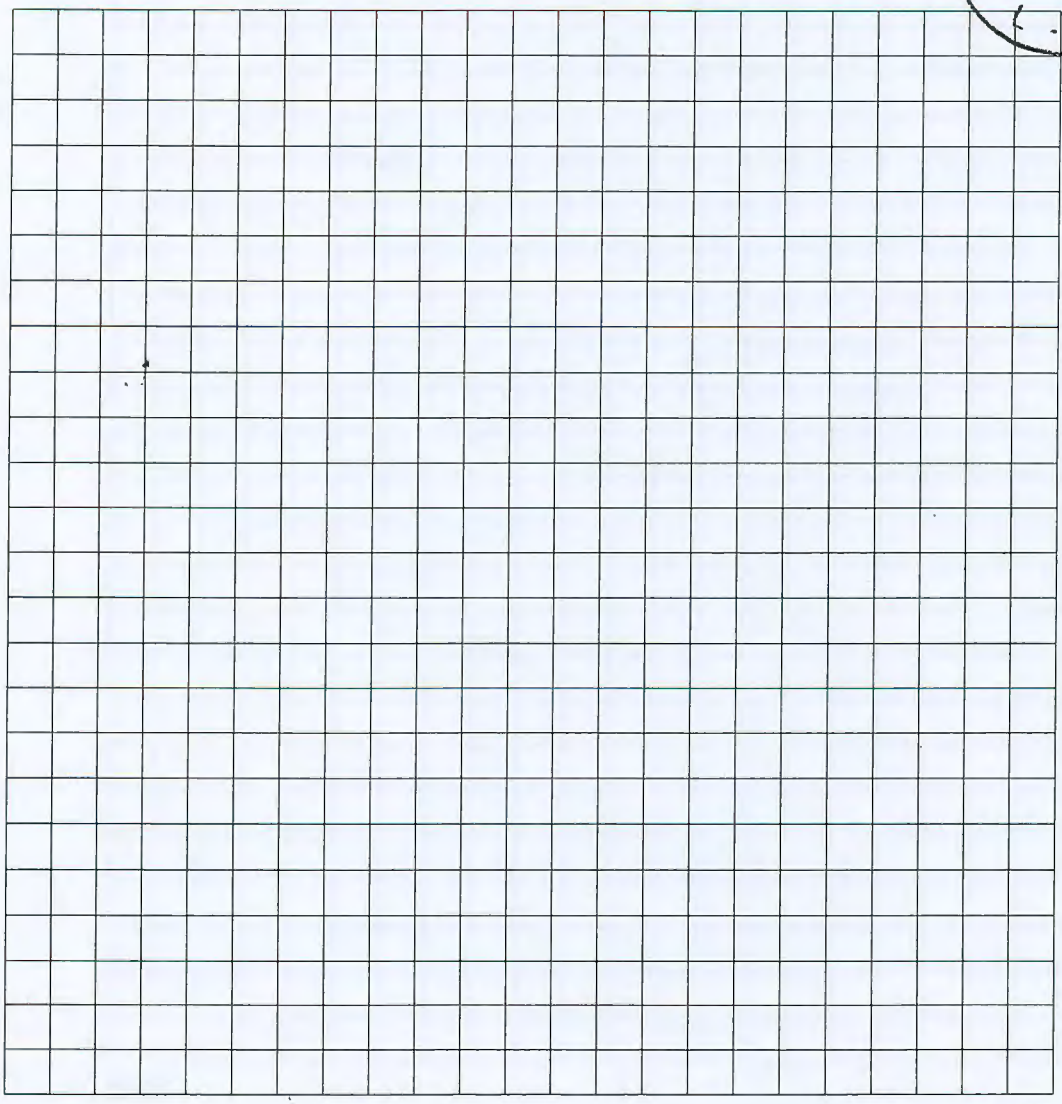
Scale: 1/4 inch = 1 foot



60SP016A
12/20/99

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1502
Fls:
Doc: 3701

Scale: 1/4 inch = 1 foot

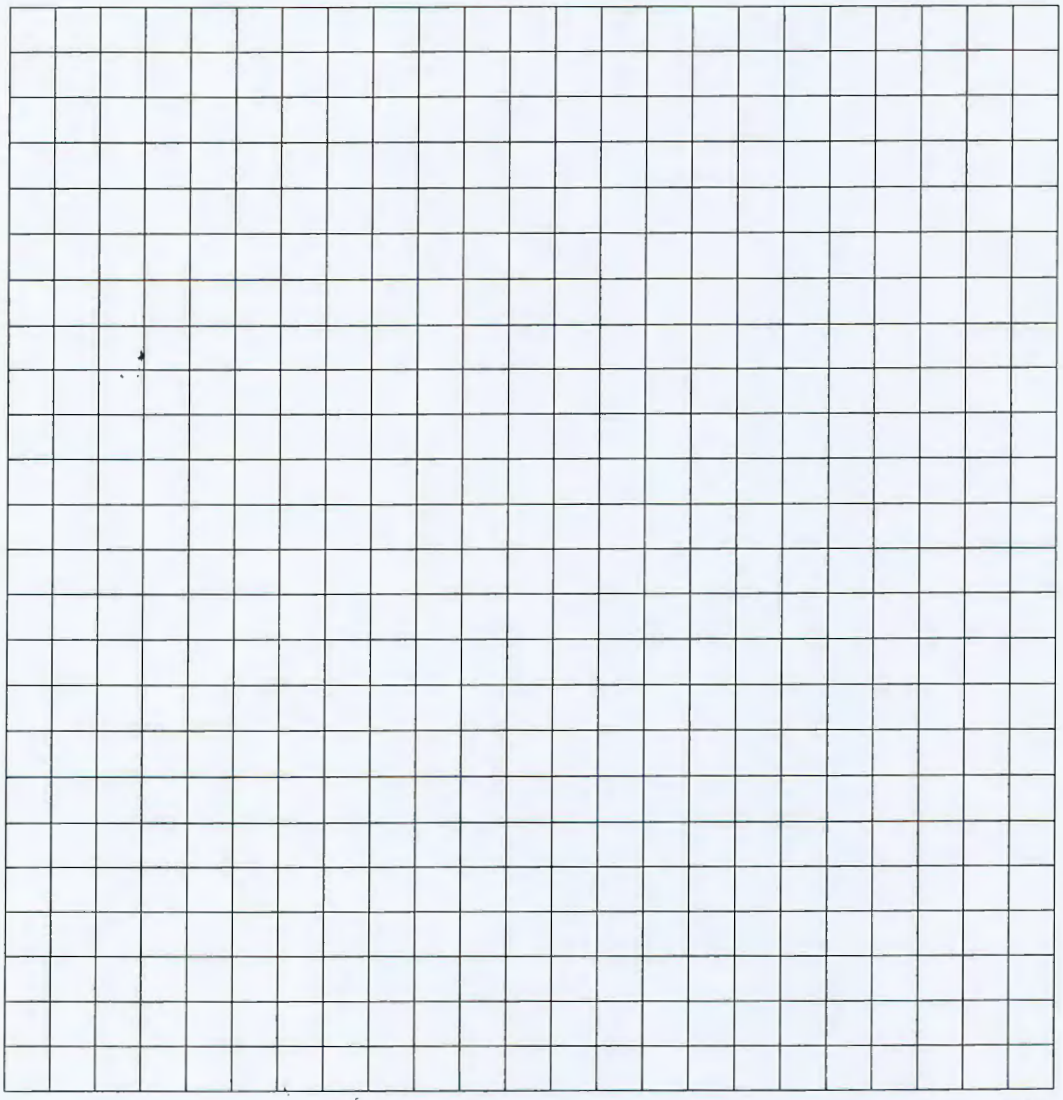


V25U067
10/2/98

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1503
Fls: 95
3701
Doc:

Computer Room Layout Plan

Scale: 1/4 inch = 1 foot



V25U067
10/2/98

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1504
Fls: 97
Doc: 3701

D Superdome LAN Interconnect Diagram

Have the customer fill in Table D-1 on page 100 with LAN information. Use the following diagram to help correlate the LAN connection with the IP address.

You will need customer-supplied LAN information for:

- Customer port on GSP

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1505
99
Fls:
Doc: 3701

- Console port on SMS
- Customer network interface on SMS (10/100 Base-T Port)
- Each network interface on each partition
- PC/Workstation console

Table D-1 LAN Information

LAN Port:	Hostname (GSP Network Name)	IP Address	Subnet Mask	Gateway Address
SD[a] GSP Private	Priv-nn (where *nn* is 01, 02, 03, ...)	192.168.2.1n (where *n* is 1, 2, 3, ...)	255.255.255.0	192.168.2.1n (where *n* is 1, 2, 3, ...)
SD Customer Port				
SMS[b] Customer Port (LAN 1, 10/100 BASE-T Port)				
SMS LAN Console				
SMS Private Port	PrivateM	192.168.2.10M (where M is 1, 2, 3, ...)	255.255.255.0	192.168.2.10M (where M is 1, 2, 3, ...)
PC/Workstation Console				
Partition 0 (Net Interface 1)				
Partition 0 (Net Interface 2)				
Partition 0 (Net Interface 3)				
Partition 1 (Net Interface 1)				
Partition 1 (Net Interface 2)				
Partition 1 (Net Interface 3)				
Partition 2 (Net Interface 1)				
Partition 2 (Net Interface 2)				
Partition 2 (Net Interface 3)				
Partition 3 (Net Interface 1)				
Partition 3 (Net Interface 2)				
Partition 3 (Net Interface 3)				
Partition 4 (Net Interface 1)				
Partition 4 (Net Interface 2)				
Partition 4 (Net Interface 3)				

Table D-1 LAN Information (Continued)

LAN Port:	Hostname (GSP Network Name)	IP Address	Subnet Mask	Gateway Address
Partition 5 (Net Interface 1)				
Partition 5 (Net Interface 2)				
Partition 5 (Net Interface 3)				

a. Superdome
b. Support Management Station

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1506
Doc: 3701

E Superdome Configurations

Table E-1 shows Superdome power requirements by configuration (i.e. number of cell boards, amount of memory per cell, and number of I/O chassis). This requirement applies to 32-way-capable systems with PA8600 or PA8700 processors.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1507
Doc: 3701

There are two columns of power numbers (Watts). The Power Breaker column shows the power used to size the wall breaker at the installation site. The Typical Power column shows typical power. Typical power numbers are for PA8600 systems and may be used to assess average utility cost of cooling and electrical power. Expect these typical numbers to be about 18% less for PA8700 systems. Table E-1 also shows the recommended breaker sizes for 4-wire and 5-wire sources.

Table E-1 Typical Superdome Configurations

Cell Boards	Memory Per Cell Board	I/O Chassis Modules	Breaker Power[a]	Recommended 3-pole Breaker Size[a,b]	Recommended 4-pole Breaker Size[a,c]	Typical Power	Typical Cooling
Qty.	GBytes	Qty.	Watts	Amps (min.)	Amps (min.)	Watts	BTU/HR
8	16	4	10660	40	25	8460	28,850
8	16	2	9600	40	25	7780	26,530
8	8	4	9220	40	25	7340	25,030
8	8	2	8160	30	20	6660	22,710
8	4	4	8500	35	20	6780	23,120
8	4	2	7440	30	20	6100	20,800
6	16	4	9040	35	20	7140	24,350
6	16	2	7980	30	20	6460	22,030
6	8	4	7960	30	20	6300	21,480
6	8	2	6900	30	20	5620	19,160
6	4	4	7420	30	20	5880	20,050
6	4	2	6360	30	20	5200	17,730
4	16	4	7420	30	20	5820	19,850
4	16	2	6360	30	20	5140	17,530
4	8	4	6700	30	20	5260	17,940
4	8	2	5640	25	20	4580	15,620
4	4	4	6340	30	20	4980	16,980
4	4	2	5280	25	20	4300	14,660
2	16	2	4740	20	20	3820	13,030
2	8	2	4380	20	20	3540	12,070
2	4	2	4200	20	20	3400	11,600

a. These numbers are valid only for the specific configurations shown. Any upgrades may require a change to the breaker size. A 5-wire source utilizes a 4 pole breaker and a 4-wire source utilizes a 3 pole breaker. *The PE (Protective Earth) ground wire is not switched.*

E - T
4915
Paulo
3
A C
I

b. An input power source supplied from a 3-pole plus protective earth (PE), 4-wire system will always be wired as 240 volts phase-to-phase, no neutral or common, plus a PE ground. Three phase input voltage (240VAC) to the equipment is connected phase-to-phase. Examples of 4 wire: 200-volt phase-to-phase, 208-volt phase-to-phase, 240-volt phase-to-phase
c. An input power source supplied from a 4-pole +PE, 5 wire system may be wired as either:

208VAC phase-to-phase voltage with a common, plus a PE ground. Three phase input voltage (208VAC) to the equipment is connected phase-to-phase. The common is *not* connected to the PDCA neutral terminal.

415VAC phase-to-phase voltage with a neutral return, plus a PE ground. Three phase input voltage (230-240VAC) to the equipment is connected phase-to-neutral. The neutral is connected to the PDCA neutral terminal. Examples of 5 wire: 208-volt phase-to-phase, 380-volt phase-to-phase, 415-volt phase-to-phase

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1508
Doc: 3701

Apêndice DQ

RQS Nº 03/2005 - C
CPMI - CORREIOS
1509
Fls:
Doc: 3791

HP-UX 11i

HP-UX advances the state of the art in enterprise UNIX®

HP-UX 11i is designed to anticipate and exceed the needs of today's enterprises as the foundation of an adaptable environment—the best enterprise UNIX just got better for both PA-RISC-based and Itanium®-based systems

Business Critical Systems

RQS Nº 03/2005 - CN
CPMI - CORREIOS
invent
Fls: 1510
Doc: 3701

In today's fast-changing world, enterprises need a computing platform that provides leading technologies, robustness, and stability. HP-UX 11i is engineered to provide these qualities.

HP-UX 11i is the best operating system (OS) to power the enterprise:

- #1 rated UNIX® operating system in the industry (DH Brown UNIX OS Review, Gartner and Butler Group—UK)

HP-UX 11i has the robustness, performance scalability, high availability, manageability, and bulletproof security required by business-critical computing.

- Proven 64-bit technology
- Stability for the long haul, even across architectures
- Adapts automatically to changing environments—always flexible
- Highly secure to protect enterprise data from damage or theft
- Most widely used high-availability solutions in the industry

Power on demand to run your enterprise

Designed from the ground up to be the best commercial UNIX operating environment for the enterprise, HP-UX 11i has been the leading enterprise UNIX OS for the last 15 years, and it continues to push the software technology envelope.

Key examples of HP's technological innovation extend the partitioning continuum and the virtual server environment of HP-UX 11i with:

- Adaptive infrastructure that, upon application failover or migration (Serviceguard), automatically adjusts system resources according to defined business priorities (Workload Manager) and can automatically activate additional CPUs when needed
- Hard and soft partitioning
- Native real-time host intrusion detection
- Dynamic code translation technology providing binary compatibility across PA-RISC and Intel® Itanium® architectures

Industry-leading applications

HP-UX 11i supports all the applications that are critical to your business. We have the support of all the key ISV applications and middleware suppliers, such as Oracle®, SAP, I2, PeopleSoft, and SAS. This means that, whatever your need, you'll find an industry-leading application solution supported by HP-UX.

Middleware and application development tools

HP-UX 11i is supported by leading middleware and application development tool providers such as BEA and Rational. Add to that integrated development environments (IDEs) from leading IDE vendors including TogetherSoft, Borland, and Sitraka, and you can count on optimal application performance. HP-UX 11i offers o complete developer ecosystem with Java™, Linux/open source, and a native development environment for faster time to deployment.

The foundation of your enterprise infrastructure

HP-UX 11i offers business-critical necessities at the highest level: the world's best combination of performance, performance scalability, availability, manageability, and security.

- Performance scalability: The efficient support of large numbers of processors provides near-linear performance scalability as processors are added.
- Single-system availability capabilities include online system tuning, online data backup, online component replacement, and automatic detection and de-allocation of at-risk components.
- Multi-system availability capabilities include automatic and bi-directional failover of business-critical data and applications over extended distances.
- Manageability tools provide role-based capability sets, the ability to manage hundreds of servers from a single browser-based console, and automatic re-allocation of system resources.
- Security fortifications include a host firewall and an intrusion-detection facility that can monitor multiple servers simultaneously.

The operating environment for worry-free computing, HP-UX 11i comes as part of four world-class operating environments, all fully integrated and tested by HP. These operating environments, ordered and supported as a single product, feature fast and easy installation and administration:

- The HP-UX 11i Foundation Operating Environment provides capabilities needed by most customers.

HP-UX 11i operating environments: components

HP-UX 11i Foundation Operating Environment

- Network drivers
- HP Apache Web server
- Ignite-UX
- Real-time host intrusion detection
- Java RTE, JDK, and JPI
- CIFS client
- CIFS server
- Servicecontrol Manager
- System Inventory Manager
- HP-UX Kernel Configuration
- Software Distributor-UX
- Netscape LDAP directory server
- PAM Kerberos
- EMS Framework
- Netscape Communicator
- Base VERITAS File System for HP-UX
- Base VERITAS Volume Manager for HP-UX

HP-UX 11i Enterprise Operating Environment (everything in the foundation OE, plus the following)

- Online JFS 3.3
- Mirrordisk/UX
- Process Resource Manager (PRM)
- Glanceplus
- OpenView Performance Agent
- Event Monitoring Services (EMS) HA monitors

HP-UX 11i Mission Critical Operating Environment (everything in the enterprise OE, plus the following)

- Serviceguard
- HP-UX Workload Manager
- Serviceguard NFS toolkit
- Enterprise Cluster Master (ECM) toolkit

- The HP-UX 11i Enterprise Operating Environment adds additional system management and high-availability capabilities.
- The HP-UX Mission Critical Operating Environment provides the highest levels of manageability and high availability, including the world's only goal-based UNIX workload manager.

Hardware platforms: PA-RISC and Intel Itanium architecture

HP-UX 11i supports two industry-leading architectures—PA-RISC and the Intel Itanium architecture.

HP-UX 11i v1 is available to run on PA-RISC. This product and platform are designed to be the workhorse that handles heavy mission-critical processing loads. HP-UX 11i v1 includes the dynamic expansion of storage components, IPv4 and IPv6 (including Mobile IP), the highest levels of security certification, virtual partitioning, workload management, and the highest levels of application availability and scaling.

HP-UX 11i v2 runs on the Intel Itanium architecture. HP and Intel jointly developed this architecture, and it promises new levels of performance and value. Now, all the operating environments are available on HP-UX 11i v2 for true enterprise readiness—and they have the same look and feel as HP-UX 11i v1, available on PA-RISC. HP-UX 11i v2 scales to 64 Intel Itanium processors and runs all the HP high-availability, security, manageability, and Internet-readiness solutions. This architecture design features explicit parallel execution to derive the best possible performance from the steadily increasing number of components in microprocessors.

Architectural compatibility

HP-UX 11i provides unparalleled compatibility across the PA-RISC and Itanium-based server platforms with complete data and application build environment (source code) compatibility. HP-UX 11i v2 even has the built-in capability to execute PA-RISC binaries on the Intel Itanium architecture via Aries dynamic code translation.

Superior Linux compatibility

HP-UX 11i provides Linux API (application programming interface) compatibility, making it easy to develop an application using the popular, economical Linux platform and then deploy it in a mission-critical environment using HP-UX 11i. And with HP-UX 11i on Itanium-based server platforms, Linux compatibility will be extended to include binary compatibility.

Summary

HP-UX 11i is designed to meet, exceed, and anticipate the needs of today's enterprises as the linchpin of an always-on and adaptable infrastructure. It has the robustness, performance scalability, high availability, manageability, and bulletproof security required by business-critical computing. HP-UX 11i is also the only operating system with a clear bridge to the next-generation Intel Itanium architecture, including data, source, and even binary compatibility across the architectures.

For more information

For more information about HP-UX 11i, please visit **www.hp.com/go/hp-ux** or call your local sales representative.

For downloads and information on HP-UX software visit **www.software.hp.com**.

ECT
São Paulo - AC
RQS Nº 03/2005 - CN
CPMI - CORREIOS
1511
Fls:
Doc: 3701

HP-UX 11i Foundation Operating Environment content (except where noted as add-on product)

Scalability
- 64 way symmetric multiprocessing scalability
- (up to 128-way by the end of 2003)
- Up to 256 gigabytes of memory
- Increasing to 1 terabyte by end of 2003)
- Terabyte maximum file system and file size
- Increasing to 4 terabytes in 2003)
- Autoport aggregation for higher networking bandwidths (add-on product)[2]
- Dynamic memory page sizing
- Instant capacity on demand (iCOD—add-on product)

Performance
- Support for high-performance PA-RISC processors
- Support for the Intel Itanium Processor Family
- 64N threads for optimal Java performance[1]

Reliability and availability
- Integrated operating environments
- Dynamic processor resilience
- Dynamic memory resilience
- Memory sparing technology
- Online file system administration (Online Journaled File System—add-on product)
- Fast file system recovery (Journaled File System)
- Disk mirroring (Mirrordisk/UX—add-on product)
- System administrator notification of system exception conditions
- Dynamically tunable kernel parameters
- Autoport aggregation for transparent link redundancy (add-on product)[2]
- Serviceguard for automatic application failover (add-on product)
- Highly available SAP and Oracle9*i* RAC environments with Serviceguard extension products (add-on products)
- Serviceguard Manager for centralized cluster management (HP-UX and Linux clusters)
- Toolkits for rapid application deployment (add-on products)
- Dynamic failover to iCOD CPUs
- Geographically Dispersed Clusters including Disaster Tolerant Solutions and Business Continuity Solutions
- Extended Campus Cluster, Metrocluster, and Continentalclusters[2]—all add-on products)

Security
- Hardened kernel
- Trusted users, passwords, disks, file systems, and permissions
- Public Key Infrastructure (PKI) support[2]
- Buffer overflow protection (transparent to applications)
- IPSec—Internet Protocol Security including OSF Application Environment Specification (AES) Encryption and Internet Key Exchange (IKE)
- Real-time host intrusion detection system
- IPFilter host firewall
- Internet daemon services
- Built-in encryption/decryption accelerators
- Netscape directory server LDAP
- LDAP-UX integration with UNIX and Windows® 2000[2]
- AAA (Authentication, Authorization, and Accounting) Server (RADIUS)
- Security Patch Check
- AAA Mobile Server (DIAMETER)
- Common Criteria EAL 4—CAPP Certified
- Pluggable Security modules
- Kerberos server (available for Itanium-based server)
- HP-UX Bastille (secure system lockdown)
- Install-time security lockdown through Bastille[1]
- Secure Shell

Connectivity and interoperability
- Industry-standard TCP/IP
- Web Services Suite
- TCP Wrappers for network activity monitoring
- SLP (Service Location Protocol)
- ARPA Services
- IPv4, IPv6
- WU-FTP (Washington University File Transfer Protocol)
- Mobile IPv4[2]
- Dynamic Host Configuration Protocol v4 and v6 (DHCP)
- Berkeley Internet Name Domain (BIND) 9.2
- Dynamic Name Service (DNS)
- Sendmail 8.11.1
- Common Internet File System (CIFS)
- Internet Express

Web application infrastructure
- HP Apache-based Web Server Suite integrated with additional HP features, including built-in Secure Sockets Layer (SSL); tuned for high performance
- BEA WebLogic Platform 7.0 including the #1 J2EE BEA WebLogic Server
- Oracle 9*i* Application Server[2]

Manageability
- Centralized management console with GUI interface (Servicecontrol Manager)
- Networkable multi-system configuration tracking (System Inventory Manager)
- Online GUI-based dynamic kernel configuration (HP-UX kernel configuration)
- Management of hundreds of remote nodes (Centralized Web Console—add-on product)
- Role-based system administrator capabilities
- Automatic system administrator notification of exception conditions (Event Monitoring Service)
- Hardware-based partitions
- Software-based partitions[2] (HP-UX Virtual Partitions—add-on product)
- Graphical user interface for creating and viewing hard partitions (Partition Manager)
- Allocation of system resources (Process Resource Manager—add-on product)
- Single-system intelligent policy engine that advises or automatically acts to provide goal-based allocation of system resources across Virtual Server Environment technologies (HP-UX Workload Manager—add-on product)
- Automatic OS updates over a network (Ignite-UX)
- Automatic application software updates over a network (Software Distributor-UX)

Linux compatibility
- GNU Tool Chain
- Over 50 Open Source tools
- Application Programming Interface (API) compatibility
- Application Binary Interface (ABI) compatibility[1] (available second half, 2003)
- Scanner to identify problems and recommended changes
- Extensive documentation on Best Practices on Porting to HP-UX 11i accessible online at **www.hp.com/go/LPK**

Application development tools
- COBOL
- Java
- C
- C++
- Fortran

Cross-architectural compatibility
- Source code compatibility (including 32-bit PA-RISC applications)
- Data compatibility
- Aries dynamic code translation technology[1]

[1] Itanium-based systems only
[2] PA-RISC-based systems only

learn more, visit www.hp.com.

Copyright 2003 Hewlett-Packard Development Company, LP. The information contained herein is subject to change without notice and is provided "as is" without warranty of any kind. The 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.

Intel, Itanium, and Itanium Processor Family are trademarks or registered trademarks of Intel Corporation in the U.S. and other countries and are used under license. Java is a U.S. trademark of Sun Microsystems, Inc. Oracle is a registered U.S. trademark of Oracle Corporation, Redwood City, California. OSF is a trademark of The Open Group in the U.S. and other countries. UNIX is a registered trademark of The Open Group. Windows is a U.S. registered trademark of Microsoft Corporation.

5981-7117EN, 05/2003

invent

Apêndice DR

ROS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1512
Doc: 3701

4 Online Backup

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1513
Doc: 3701

Introduction

This chapter describes the online backup facility provided with the VxFS file system. The snapshot feature of VxFS can be used to create a snapshot image of a mounted file system, which becomes a duplicate read-only copy of the mounted file system.

NOTE Snapshot file systems are available only with the optional HP OnLineJFS product.

The following topics are covered in this chapter:

- "Snapshot File Systems"
  - — "Snapshot File System Disk Structure"
  - — "How a Snapshot File System Works"
- "Using a Snapshot File System for Backup"
  - — "Creating a Snapshot File System"
  - — "Making a Backup"
- "Performance of Snapshot File Systems"

Snapshot File Systems

The VxFS file system provides a mechanism for taking snapshot images of mounted file systems, which is useful for making backups.The *snapshot file system* is an exact image of the original file system, which is referred to as the *snapped file system*. The snapshot is a consistent view of the file system "snapped" at the point in time the snapshot is made. Selected files can be backed up from the snapshot (using standard utilities such as `cpio` or `cp`) or the entire file system image can be backed up (using the `vxdump` or `fscat` utilities).

The `mount` command is used to create a snapshot file system; there is no `mkfs` step involved. A snapshot file system is always read-only and exists only as long as it and the file system that has been snapped are mounted. A snapped file system cannot be unmounted until any corresponding snapshots are first unmounted. A snapshot file system ceases to exist when unmounted. While it is possible to have multiple snapshots of a file system made at different times, it is not possible to make a snapshot of a snapshot.

This chapter describes the creation of snapshot file systems and gives some examples of backing up all or part of a file system using the snapshot mechanism.

Snapshot File System Disk Structure

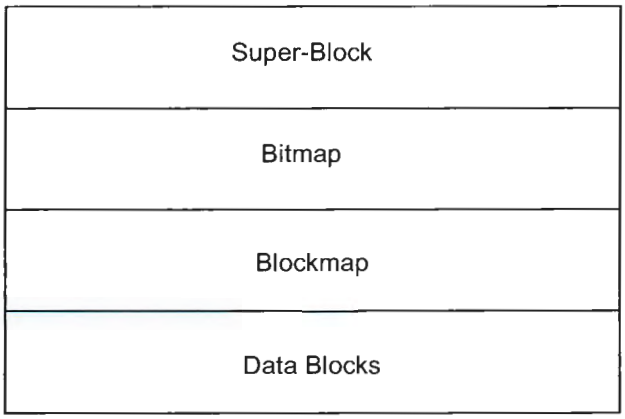
A snapshot file system consists of:

- a super-block
- a bitmap
- a blockmap
- data blocks copied from the snapped file system

Figure 4-1, "The Snapshot Disk Structure," shows the disk structure of a snapshot file system.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1514
Fls:
3701
Doc:

Figure 4-1 **The Snapshot Disk Structure**



The super-block is similar to the super-block ofa normal VxFS file system, however, the magic number is different and many of the fields are meaningless.

Immediately following the super-block is the bitmap. The bitmap contains one bit for every block on the snapped file system. Initially, all bitmap entries are zero. A set bit indicates that the appropriate block was copied from the snapped file system to the snapshot. In this case, the appropriate position in the blockmap will reference the copied block,

Following the bitmap is the blockmap. It contains one entryfor each block on the snapped file system. Initially, all entries are zero. When a block is copied from the snapped file system to the snapshot, the appropriate entry in the blockmap is changed to contain the block number on the snapshot file system that holds the data from the snapped file system.

The data blocks used by the snapshot file system are located after the blockmap. These are filled by any data copied from the snapped file system, starting from the front of the data block area.

How a Snapshot File System Works

A snapshot file system is created by mounting an empty disk slice as a snapshot of a currently mounted file system. The bitmap, blockmap and super-block are initialized and then the currently mounted file system is frozen (see "Freeze and Thaw", for a description of the VX_FREEZE ioctl). Once the file system to be snapped is frozen, the snapshot is enabled and mounted and the snapped file system is thawed. The snapshot appears as an exact image of the snapped file system at the time the snapshot

E C T
4909
Paulo
C P L - A C

HP JFS 3.3 and HP OnLineJFS 3.3 VERITAS File System 3.3 System Administrator's Guide

for HP-UX 11.00 and HP-UX 11i

November, 2000

HP 9000 Systems

Manufacturing Part Number: B3929-90011
E1100

United States

© Copyright 1983-2000 Hewlett-Packard Company. All rights reserved..

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1515
Fls:
3701
Doc:

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 and any supporting software media (CD-ROMs, flexible disk, and tape cartridges) 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 Notices

Copyright © 1983-2000 Hewlett-Packard Company. All rights reserved. Reproduction, adaptation, or translation of this document without prior written permission is prohibited, except as allowed under the copyright laws.

Copyright © 1979, 1980, 1983, 1985-93 Regents of the University of California. This software is based in part on the Fourth Berkeley Software Distribution under license from the Regents of the University of California.

Copyright © 1988 Carnegie Mellon University
Copyright © 1990-1995 Cornell University
Copyright © 1986 Digital Equipment Corporation.
Copyright © 1997 Isogon Corporation
Copyright © 1985, 1986, 1988 Massachusetts Institute of Technology.
Copyright © 1991-1997 Mentat, Inc.
Copyright © 1996 Morning Star Technologies, Inc.
Copyright © 1990 Motorola, Inc.
Copyright © 1980, 1984, 1986 Novell, Inc.
Copyright © 1989-1993 The Open Software Foundation, Inc.
Copyright © 1996 Progressive Systems, Inc.
Copyright © 1989-1991 The University of Maryland
Copyright © 1986-1992 Sun Microsystems, Inc.

Trademark Notices

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.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1516
Doc: 3701

Contents

1. **The VxFS File System**

Introduction 18

JFS 3.3 and OnLineJFS 3.3 Product Availability 19

JFS and OnLineJFS Feature Comparison 20

Disk Layout Options 21
- Version 2 21
- Version 3 21
- Version 4 21

File System Performance Enhancements 22

Extent-Based Allocation 23
- Typed Extents 24

Extent Attributes 26

Fast File System Recovery 27

Online System Administration 28
- Defragmentation 28
- Resizing 29

Online Backup 30

Application Interface 31
- Application Transparency 31
- Expanded Application Facilities 31

Extended mount Options 32
- Enhanced Data Integrity Modes 32
- Enhanced Performance Mode 33
- Temporary File System Modes 33
- Improved Synchronous Writes 33

Enhanced I/O Performance 35
- Enhanced I/O Clustering 35

E C T 4905 Paula AC
RQS Nº 03/2005 - CN
CPMI - CORREIOS
1517
Fls:
Doc: 3701

ECT 1994 Paris CPL - AC

Contents

Application-Specific Parameters 35
Quotas 37
Access Control Lists 38
Support for Large Files 39
Creating a File System with Large Files 39
Mounting a File System with Large Files 39
Managing a File System with Large Files 40

2. Disk Layout

Introduction 42
Disk Space Allocation 44
The VxFS Version 1 Disk Layout 45
Overview 45
Super-Block 46
Intent Log 46
Allocation Unit 47
The VxFS Version 2 Disk Layout 51
Overview 51
Basic Layout 52
Filesets and Structural Files 57
Locating Dynamic Structures 66
The VxFS Version 3 Disk Layout 68
The VxFS Version 4 Disk Layout 71

3. Extent Attributes

Introduction 74
Attribute Specifics 75
Reservation: Preallocating Space to a File 75

Contents

E C T
2903
Paula
C P L - A C

Fixed Extent Size 76
Other Controls 77

Commands Related to Extent Attributes 79
Failure to Preserve Extent Attributes 80

4. Online Backup

Introduction 82

Snapshot File Systems 83
Snapshot File System Disk Structure 83
How a Snapshot File System Works 84

Using a Snapshot File System for Backup 87
Creating a Snapshot File System 87
Making a Backup 88

Performance of Snapshot File Systems 90

5. Performance and Tuning

Introduction 92

Choosing a Block Size 93

Choosing an Intent Log Size 94

Choosing Mount Options 95
log 95
delaylog 95
tmplog 96
nolog 96
nodatainlog 96
blkclear 96
mincache 97
convosync 98

ROS Nº 03/2005 - CN
CPMI - CORREIOS
1518
Fls:
3701
Doc:

C T
São Paulo
CPL - AC

Contents

Combining mount Options 99

Kernel Tuneables 101
Internal Inode Table Size 101

Monitoring Free Space 102
Monitoring Fragmentation 102

I/O Tuning 105
Tuning VxFS I/O Parameters 105
Tuneable VxFS I/O Parameters 105

6. Application Interface

Introduction 110

Cache Advisories 111
Direct I/O 111
Unbuffered I/O 112
Discovered Direct I/O 112
Data Synchronous I/O 112
Other Advisories 113

Extent Information 114
Space Reservation 114
Fixed Extent Sizes 116
Freeze and Thaw 117

Get I/O Parameters ioctl 118

7. Quotas

Introduction 120

Quota Limits 121

Quotas File on VxFS 122

Quota Commands 123

Contents

quotacheck With VxFS 123
Using Quotas 124

A. Kernel Messages

Introduction 128
File System Response to Problems 129
Marking an Inode Bad 129
Disabling Transactions 129
Disabling the File System 129
Recovering a Disabled File System 129
Kernel Messages 131
Global Message IDs 131

Glossary

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1519
Doc: 3701

E C T
4899
São Paulo
AC

Preface

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1520
Fls: 3701
Doc:

Introduction

The *VERITAS© File System System Administrator's Guide* provides information on the most important aspects of administering a VERITAS File System™ (VxFS©).The VERITAS File System is also known as the Journaled File System, or JFS. This guide also provides information on administering the HP OnLineJFS product, an optional add-on product for HP-UX systems. This document describes JFS 3.3 and OnLineJFS 3.3.

This guide is for system administrators who configure and maintain HP-UX 11.x systems with JFS 3.3, and assumes that you have:

- An understanding of system administration.
- A working knowledge of the HP-UX operating system.
- A general understanding of file systems.

E C T
4897
Paula
I
AC

Organization

- Chapter 1, The VxFS File System,, introduces the features and characteristics of this product.
- Chapter 2, Disk Layout, describes and illustrates the major components of VxFS disk layouts.
- Chapter 3, Extent Attributes, describes the policies associated with allocation of disk space.
- Chapter 4, Online Backup, describes the snapshot backup feature of VxFS.
- Chapter 5, Performance and Tuning, describes VxFS tools that optimize system performance. This section includes information on mount options.
- Chapter 6, Application Interface, describes ways to optimize an application for use with VxFS. This chapter includes details on cache advisories, extent sizes, and reservation of file space.
- Chapter 7, Quotas, describes VxFS methods to limit user access to file and data resources.
- Appendix A, Kernel Messages, lists VxFS kernel error messages in numerical order and provides explanations and suggestions for dealing with these problems.
- The "Glossary" contains a list of terms and definitions relevant to VxFS.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1521
Fls:
3701
Doc:

Related Documents

To install JFS 3.3 and OnLineJFS 3.3, and for more information about these products, see the following documents:

- For HP-UX 11.00 systems: *HP JFS 3.3 and HP OnLineJFS 3.3 Release Notes*
- For HP-UX 11.10 systems: *Release Notes for HP-UX Release 11.10 and HP-UX 11.10 Installation and Configuration Notes*
- For HP-UX 11i systems: *HP-UX 11i Release Notes* and *HP OnLineJFS 3.3 Release Notes for HP-UX 11i*

The online manual pages provide additional details on VxFS commands and utilities.

E C T
4895
Paula
L - AC

Conventions

Typeface	Usage	Examples
monospace	computer output, files, directories, software elements such as command options, function names, and parameters	Read tuneables from the `/etc/vx/tunefstab` file. See the `ls`(1) manual page for more information.
`monospace (bold)`	user input	**`# mount -F vxfs /h/filesys`**
italic	new terms, book titles, emphasis, variables replaced with a name or value	See the *User's Guide* for details. The variable *ncsize* determines the value of...

Symbol	Usage	Examples
%	C shell prompt	
$	Bourne/Korn shell prompt	
#	superuser prompt (all shells)	
\	continued input on the following line; you do not type this character	**`# mount -F vxfs \ /h/filesys`**
[ ]	in a command synopsis, brackets indicates an optional argument	`ls [ -a ]`
|	in a command synopsis, a vertical bar separates mutually exclusive arguments	`mount [ suid | nosuid ]`

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1522
Fls: 3701
Doc:

Technical Support

For license information contact Hewlett-Packard World Wide Licensing Services:

California, U.S.A.
Phone: 650-960-5111
fax: 650-960-5670
e-mail: hplicense@mayfield.hp.com
Hours: Monday through Friday, 8am-5pm PST

Grenoble, France
Phone: +33.(0)4.76.14.15.29
fax: +33.(0)4.76.14.25.15
e-mail: codeword_europe@hp-france-gen1.om.hp.com
Hours: Monday through Friday, 8am-5pm GMT +1

For technical support, if you have a support contract, call the HP Response Center at 1-800-633-3600.

For additional information about HP OnLineJFS and other HP high availability products, visit the Web site at:

www.hp.com/go/ha

E C T I
4893
Paula
L - AC

1 The VxFS File System

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1523
Fls: 3701
Doc:

ECT
1892
Poujol
CPL - AC

Introduction

VxFS is an extent based, intent logging file system. VxFS is particularly geared toward UNIX environments that require high performance and availability and deal with large volumes of data.

This chapter provides an overview of major VxFS features that are described in detail in later chapters.The following topics are covered in this chapter:

- "JFS and OnLineJFS Feature Comparison"
- "Disk Layout Options"
- "File System Performance Enhancements"
- "Extent-Based Allocation"
- "Extent Attributes"
- "Fast File System Recovery"
- "Online System Administration"
- "Online Backup"
- "Application Interface"
- "Extended mount Options"
- "Enhanced I/O Performance"
- "Quotas"
- "Access Control Lists"
- "Support for Large Files"

JFS 3.3 and OnLineJFS 3.3 Product Availability

HP JFS 3.3 and HP OnLineJFS 3.3 are available for HP-UX 11.00 and later systems. You can download JFS 3.3 for HP-UX 11.00 for free from the HP Software Depot (http://www.software.hp.com), or you can request a free JFS 3.3 CD from the Software Depot. You can purchase HP OnLineJFS 3.3 (product number B3929CA for servers and product number B5118CA for workstations) for HP-UX 11.0 or HP-UX 11i from your HP sales representative. JFS 3.3 is included with HP-UX 11i systems.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1524
Doc: 3701

E C 1
1990
CPL - AC

JFS and OnLineJFS Feature Comparison

HP-UX supports two separate Journaled File System products: the basic product, JFS, which is built into the HP-UX operating system, and the optional, advanced product, OnLineJFS, which is purchased separately. The following table lists VxFS file system features supported in JFS 3.3 and OnLineJFS 3.3.

Table 1-1 VxFS File System Feature Comparison

Feature	JFS 3.3	OnLineJFS 3.3
extent-based allocation	*	*
extent attributes	*	*
fast file system recovery	*	*
access control list (ACL) support	*	*
enhanced application interface	*	*
enhanced mount options	*	*
improved synchronous write performance	*	*
support for large files (up to one terabyte)	*	*
support for large file systems (up to one terabyte)	*	*
enhanced I/O performance	*	*
support for BSD-style quotas	*	*
unlimited number of inodes	*	*
file system tuning [`vxtunefs`(1M)]	*	*
online administration		*
ability to reserve space for a file and set fixed extent sizes and allocation flags		*
online snapshot file system for backup		*
direct I/O, supporting improved database performance		*
data synchronous I/O		*
DMAPI		*

VxFS supports all UFS file system features and facilities except for the linking, removing, or renaming of "." and ".." directory entries. Such operations may disrupt file system sanity.

Disk Layout Options

Three disk layout formats are available with VxFS:

Version 2

The Version 2 disk layout supports such features as:

- filesets
- dynamic inode allocation

The Version 2 layout is available with optional support for quotas.

Version 3

The Version 3 disk layout offers additional support for:

- files up to one terabyte
- file systems up to one terabyte

Version 4

Version 4 is the latest disk layout with the following additional feature:

- Access Control Lists

See Chapter 2 , "Disk Layout" for a description of the disk layouts.

The following table lists HP-UX Releases with the VxFS versions and disk layouts they support:

Table 1-2 Supported and Default Disk Layouts on HP-UX Releases

HP-UX Release	VxFS Version	Supported Disk Layouts	Default Disk Layout
10.10	2.3	2	2
10.20	3.0	2, 3	3
11.00 with JFS 3.1	3.1	2, 3	3
11.00 with JFS 3.3	3.3	2, 3, 4	3
11i	3.3	2, 3, 4	4

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1525
Fls:
3701
Doc:

File System Performance Enhancements

The HFS file system uses block based allocation schemes which provide adequate random access and latency for small files but limit throughput for larger files. As a result, the HFS file system is less than optimal for commercial environments.

VxFS addresses this file system performance issue through an alternative allocation scheme and increased user control over allocation, I/O, and caching policies. An overview of the VxFS allocation scheme is covered in the section "Extent-Based Allocation".

VxFs provides the following performance enhancements:

- extent based allocation
- enhanced mount options
- data synchronous I/O
- direct I/O and discovered direct I/O
- caching advisories
- enhanced directory features
- explicit file alignment, extent size, and preallocation controls
- tuneable I/O parameters
- tuneable indirect data extent size

The rest of this chapter along with Chapter 5 , 'Performance and Tuning" and Chapter 6 , "Application Interface" provide more details on some of these features.

Apêndice DS

REG Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1528
Doc: 3701

E C T
4843
Paula
C & L - AC

User Guide

rp5400 Family of Servers

First Edition

Manufacturing Part Number : A5191-96018
November 2002

USA

© Copyright 2002

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1527
Fls:
3701
Doc:

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.

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.

Copyright Notices. ©copyright 1983-2002 Hewlett-Packard Company, all rights reserved.

Windows", Windows NT", Windows 95", Windows 2000", and Windows XP" are registered trademarks of Microsoft in the U.S. and other countries.

Reproduction, adaptation, or translation of this document without prior written permission is prohibited, except as allowed under the copyright laws.

Contents

1. Server Overview

2. Server Unpacking and Installation

Factory Integrated rp54xx Cabinet Installation 4
Receive and Unpack A Non-Integrated Server 7
Unpacking the server 7
Install Deskside Server 10
Install Stand-Alone Server in a Cabinet. . . . 13
Stationary L-Bracket Rail Assembly 19
Identifying Approved Non-E-Series HP Cabinets. . . . 19
Identifying E-Series HP Cabinets 20
Identifying Static Rail Kit 20
Installing Stationary Rails. . . . 21

3. Installing Additional Components

Additional Components 24
Installing Memory 25
Memory Configuration Rules. . . . 25
Installing Peripheral Component Interconnect (PCI) Cards. . . . 30
rp5400/rp5450 PCI Card Slots. . . . 30
rp5470 PCI Card Slots 31
PCI I/O Card Installation Restrictions 32
PCI I/O Card Installation Order 32
Installing a PCI Card 34
Online Addition/Replacement (OLA/R) of PCI I/O cards 36
Installing Graphics 37
Graphics Troubleshooting 43
Installing Disk Drives 44

4. Cable Connections

Core I/O Connections. . . . 48
Revision A GSP. . . . 48
Revision B GSP. . . . 49
Guardian Service Processor (GSP) Overview. . . . 51
GSP LAN. . . . 51
GSP RS-232. . . . 51
GSP Features 51
Revision A GSP. . . . 52
Revision B GSP. . . . 52
Configure System Consoles. . . . 53
GSP Cables 54
Configure RS-232 Console 54
Configure Remote Console 58
Configure the LAN Console 59
Configure the Web Console 61
Secure Web Console Installation. . . . 66

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1528
Doc: 3701

GSP Configurable Parameters 69
Adding Users 69
Removing Users 70
Return the GSP to Default Configurations 71
rp54xx Server Boot Process 72
Initial Power-up 74

5. Utilities

Configuring the Rev A Guardian Service Processor (GSP) 78
Configuring the GSP LAN Port 78
Adding Users 78
Removing Users 80
Changing the Default GSP Configuration 80
Configuring the Rev B Guardian Service Processor (GSP) 81
Configuring the GSP LAN Port 81
Adding Users 81
Removing Users 83
Changing the Default GSP Configuration 83

6. Troubleshooting

Determine Current System State 86
Troubleshooting and FRU identification 87
Problem Symptoms and Repair Actions 87
Chassis Code to FRU Decode 91
Cross-Referencing Chassis Log Errors to rp54xx FRUs 91
Interpreting System Alerts 94
Interpreting Service Processor Error Chassis Logs 96
Interpreting Chassis Logs Using the chassis_code.codes File 98
rp5400 and rp5450 System Block Diagram 100
rp5400 and rp5450 I/O Block Diagram 101
rp5430 and rp5470 System Block Diagram 102
rp5430 and rp5470 I/O Block Diagram 103
Run/Attention/Fault LED States 104
PCI I/O LED States 112
Expansion I/O LED States 114
GSP LED States 116
LAN/SCSI LED States 118
Fan, Power Supply, and Disk LED States 119

7. Removing and Replacing Components

List of Changeable Parts with Remove and Replace Components 122
Cardcage Fan 122
Core I/O 122
HotSwap Chassis Fan 122
Disk Drive 123
Display Board 123

Front Bezel 123
Memory DIMM 123
PCI I/O Card 124
Power Supply 124
HotSwap Power Converter Fan 124
Platform Monitor 124
Processor Support Module 125
Individual Component Remove/Replace Instructions 126
Extend the Server out the Front 126
Insert the Server from the Front 127
Stand-alone Server Cover Removal 128
Stand-alone Server Cover Replacement 130
Top Cover Removal 131
Top Cover Replacement 132
Side Cover Removal 133
Side Cover Replacement 134
Front Bezel Removal (Single Piece) 135
Front Bezel Replacement (Single Piece) 136
Front Bezel Removal (Two Piece) 137
Front Bezel Replacement (Two Piece) 138
Core I/O Removal 139
Core I/O Replacement 140
PCI Card Separator/Extractor Removal 142
PCI Card Separator/Extractor Replacement 143
HotPlug Disk Drive Removal 144
HotPlug Disk Drive Replacement 149
HotSwap Chassis Fan Cover Removal 152
HotSwap Chassis Fan Cover Replacement 153
HotSwap Chassis Fan Removal 154
HotSwap Chassis Fan Replacement 155
HotSwap Card Cage Fan Removal 156
HotSwap Card Cage Fan Replacement 157
HotSwap Power Supply Removal 158
HotSwap Power Supply Replacement 159
HotSwap Power Converter Fan Removal 160
HotSwap Power Converter Fan Replacement 161
Processor Support Module Removal 162
Processor Support Module Replacement 163
Memory DIMM Removal 164
Memory DIMM Replacement 165
Display Board Removal 166
Display Board Replacement 167
Platform Monitor Removal 168
Platform Monitor Replacement 170
PCI I/O Card Removal 172
PCI I/O Card Replacement 173

ECT 4839 Paula CPL AC

RQS Nº 03/2005 - CN
CPML - CORREIOS
15/29
Fls: 3701
Doc:

Contents

A. Parts and Accessories

CRU Physical Location 176
Customer Replaceable Unit Part Numbers 179

B. System Specifications

Dimensions 182
Uncrating Space 182
Space Requirements 182
Computer Room Physical Space Requirements 183
Computer Room Unpacking Space 184
Electrical 185
Office High Availability Requirements 185
Power Protection 185
Modular PDUs 186
System Power Requirements 186
LAN and Telephone 187
Acoustic Safety Standards 188
Altitude Operation Standards 189
Effects of Altitude 189
Temperature and Humidity Operating Standards 190
Thermal Protection Features 190

C. General Site Preparation Guidelines

Electrical Factors 192
Computer Room Safety 192
Power Consumption 193
Electrical Load Requirements (Circuit Breaker Sizing) 193
Power Quality 193
Distribution Hardware 194
Grounding Systems 195
System Installation Guidelines 197
Environmental Elements 198
Computer Room Preparation 198
Cooling Requirements 198
Humidity Level 200
Dust and Pollution Control 200
Metallic Particulate Contamination 201
Electrostatic Discharge (ESD) Prevention 202
Acoustics 202
Facility Characteristics 203
Floor Loading 203
Windows 205
Space Requirements 206
Delivery Space Requirements 206
Operational Space Requirements 206
Floor Plan Grid 206

ECT
1837
Paula
CPL - AC

Contents

Typical Installation Schedule 207
Site Inspection 208
Delivery Survey 212

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1530
Fls:
Doc: 3701

Table 6-1. Problem Symptoms and Repair Actions 87
Table 6-2. Chassis Log Error to FRU Decoder 91
Table A-1. Exchange CRUs 179
Table A-2. Non-Exchange CRUs 180
Table B-1. Power Requirements 186
Table C-1. Effect of Humidity on ESD Charge Levels 202
Table C-2. Floor Loading Term Definitions 203
Table C-3. Typical Raised Floor Specifications. 204
Table C-4. Customer and Hewlett-Packard Information 208
Table C-5. Site Inspection Checklist 209

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1531
Fls:
3701
Doc:

E C T
CPL - AC
1833
Paulo

Figures

Figure A-1. Server Rear View 176
Figure A-2. Side Service Bay 177
Figure A-3. System Board (Access via Top Service Bay) 177
Figure A-4. Server Front 178
Figure C-1. Raised Floor Metal Strip Ground System 196
Figure C-2. Delivery Survey (Part 1) 213
Figure C-3. Delivery Survey (Part 2) 214

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1538
Fls:
Doc: 3791

ECT
4831
Paulo
SPL - AC

Preface

Printing History

The Printing History below identifies the edition dates of this manual. Updates are made to this publication on an unscheduled, *as needed*, basis. The updates will consist of a complete replacement manual and pertinent on-line or CD-ROM documentation.

First Edition ..... November 2002

What's New?

The, *Upgrade Guide,rp5400 Family of Servers*, is new and was developed to provide customers with system maintenance information for those components called customer replaceable units (CRUs). Maintenance of CRUs does not require HP customer engineering services, except when specifically cautioned. The cautions are shown primarily to protect customer product warrantees.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1532
Fls: 3701
Doc:

ECT
4829
Paula
CPL - AC

1 Server Overview

The rp5400 family of servers are 1-way to 4-way servers based on the PA-RISC processor architecture. The rp5400 family of servers accommodate up to 16GB of memory and internal peripherals including disks and DVD ROM/Tape. High availability features include HotSwap fans and power supplies, and HotPlug internal disk drives. The supported operating system is HP-UX.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1534
Fls:
3701
Doc:

E C T
4827 Paula
CPL - AC

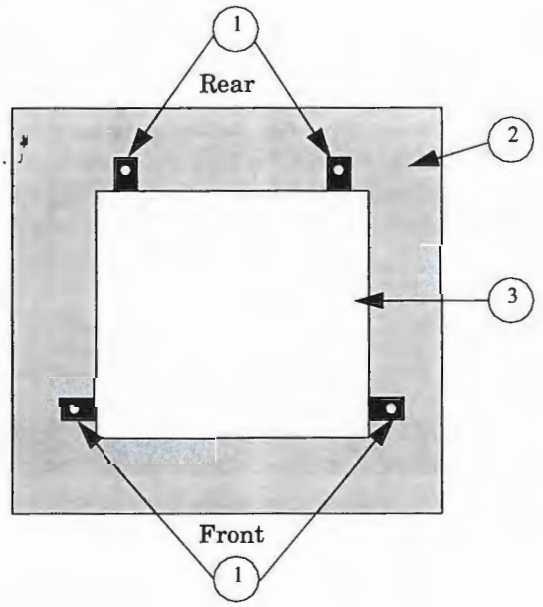
2 Server Unpacking and Installation

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1585
Doc:
3701

Factory Integrated rp54xx Cabinet Installation

A factory integrated server is one in which the rp54xx server and associated components are pre-assembled and shipped from the factory already installed in a Hewlett-Packard E-Series cabinet. Factory integrated systems reduce the amount of time required to set-up and begin server operation.

1. Carefully remove the carton and anti-static bag from the pallet.
2. Remove the front two (2) L-brackets. Retain the 1/2-inch bolts for later use.



1. Shipping L-Bracket
2. Shipping Pallet
3. Cabinet (Top View)

NOTE As viewed from the front, one bracket is located on each side at the base of the cabinet near the front.

3. At the rear of the cabinet:
   a. Open the door.
   b. Remove the anti-tip foot by removing and retaining the two (2) 1/2-inch bolts.

For Shipping: L-brackets are mounted behind anti-tip foot. Same bolts secure both.

   c. Remove the two (2) L-brackets (revealed by removing the anti-tip foot).
4. Remove the two ramps from the pallet and carefully place them into the slots at the front of the pallet.

WARNING **Use extreme care when rolling the racked system down the ramps. A rack containing one rp54xx can weigh up to 418 lbs. Do not stand in front of the ramps when rolling the cabinet off the pallet or injury may occur. All but the smallest configurations require two persons to safely remove the rack from the pallet.**

If anti-tip feet or ballast are not installed or are improperly installed the cabinet can tip. Failure to follow this precaution can cause injury to personnel or damage to equipment.

ROS Nº 03/2005 - CN - CPMI - CORREIOS
1536
Fls:
3701
Doc:

5. Straighten the rollers on the cabinet base, if needed, and carefully roll it down the ramps.

WARNING ***After removing the server from the pallet, Do not move the cabinet unless the anti-tip feet are installed!*** **The cabinet can tip if care is not used. Due to their low ground clearance the feet may catch on irregularities on the floor, thresholds, or ramps.**

Do not move the cabinet without first installing the anti-tip feet. **The cabinet may tip if moved without the anti-tip feet or ballast installed.**

Do not move the cabinet after installing the anti-tip feet unless they are in the fully-raised position. **Once installed, the anti-tip feet must be fully raised to allow ground clearance.**

Because of their low ground clearance, the fully-raised anti-tip feet may need to be removed *temporarily* to clear some obstacles such as door jambs, ramps, and other large irregularities or obstructions on the floor.

If you must temporarily remove the anti-tip feet to clear an obstacle, use extreme caution when moving the cabinet. Always reinstall the anti-tip feet as soon as the obstacle has been cleared.

Lower and secure both the anti-tip feet and the cabinet leveling/stabilizer feet once the cabinet is in place.

Failure to follow these precautions can result in equipment damage or personal injury.

6. Install the front and rear anti-tip feet using the 1/2 inch bolts provided. Ensure that the anti-tip feet are installed in the fully up position in the mounting slots. This will provide maximum ground clearance while moving the cabinet to its final position.
7. Carefully move the cabinet to its installation location.
8. Lower the anti-tip feet to the fully down position and adjust the cabinet leveling feet for best cabinet stability.

E C T
CPL - AC
4823
Paulo

Receive and Unpack A Non-Integrated Server

WARNING **The typical rp54xx system can weigh up to 68kg (150lbs). *HP recommends using an an approved lifting device.* Lift and move the server in accordance with all local safety regulations. Failure to follow this precaution can cause injury to personnel or damage to equipment.**

Unpacking the server

The following procedure describes the steps involved in unpacking the server, whether to function as a stand-alone Deskside unit, or to be integrated into a cabinet.

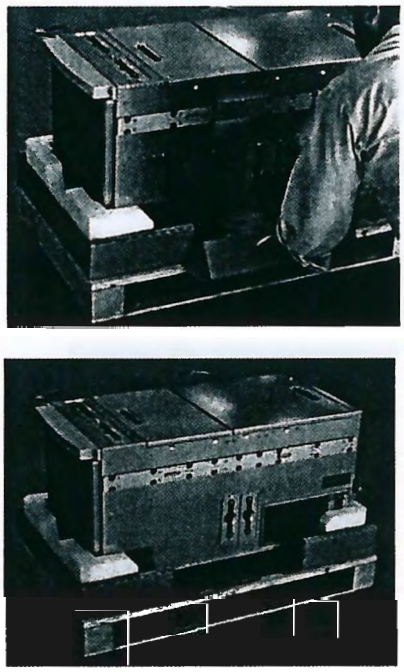
Step 1. Remove the shipping carton and anti-static bag from the server as depicted below.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1537
Fls:
3701
Doc:

NOTE The packaging for rp74xx and rp54xx servers is the same, rp74xx is shown.

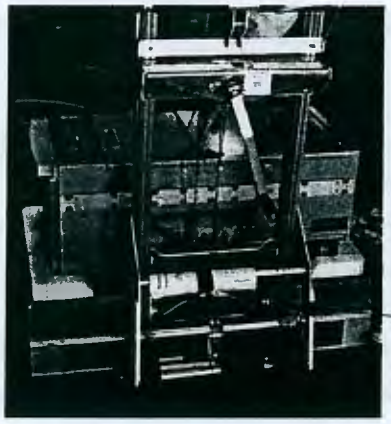
Step 2. If you are moving the server manually, use three people to lift the server from the packing material and pallet. Carefully move the server to the selected location.

Step 3. If you are moving the server by an approved lifting device (such as Genie Lift ™), remove the tear flap from the front lip of the carton bottom to allow access to the server, as illustrated below. Removal of the tear flap will reveal a slot between the bottom of the server and the inside bottom of the cardboard box.



CPL - AC

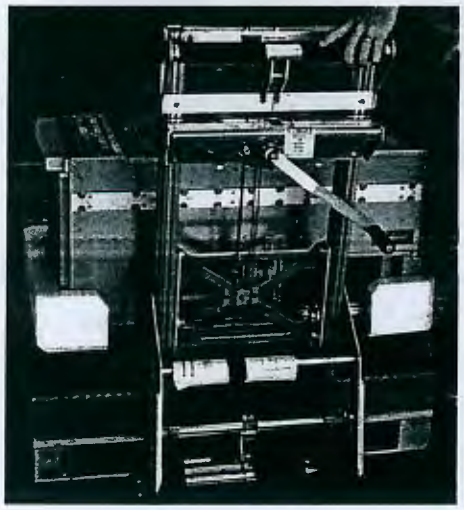
Step 4. Carefully raise the lift's platform so that it will slide into the slot located ***under*** the center of the server, but ***over*** the top of the pallet.



Lifting Device Platform.

NOTE The server's center of gravity will vary with the hardware configuration, but it is generally located slightly behind the middle of the server.

Step 5. Raise the lifting device platform enough for the server to clear the pallet and packing materials, as show below.



RQS Nº 03/2005 - CN
CPMI - CORREIOS
1538
Fls:
3701
Doc:

Install Deskside Server

The following section describes the installation of a server into a Deskside enclosure for installation in an office environment.

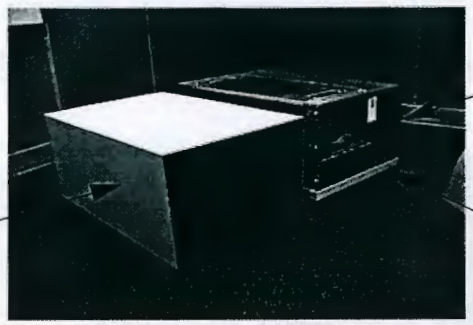
WARNING **The typical rp54xx system can weigh up to 68kg (150lbs). *HP recommends using an approved lifting device.***

- **Lift and move the server in accordance with all local safety regulations.**
- **Do not attempt to lift the server by the plastic handles on the top and side covers.**

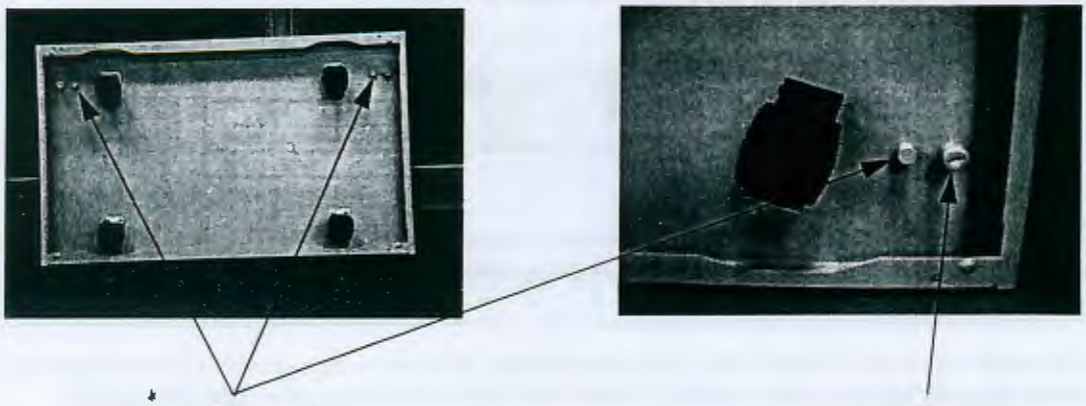
Failure to follow these precautions can cause injury to personnel or damage to equipment.

Step 1. Unpack the server.

Step 2. Unpack the deskside enclosure.



NOTE Ensure that the positioning spring pins in the enclosure base align with the alignment holes in the bottom of the server.



Step 3. Position the server on the wheeled enclosure base.

Step 4. Tighten the two captive screws in the enclosure base to secure the server to the base.

Step 5. Position the enclosure cover (outside skin) over the server and install and tighten the screws to secure it to the base.

NOTE The perforations and the lip of the outside skin should be toward the rear of the server.

WARNING **Stacking rp54xx servers in deskside enclosures is *not* supported.**

Stacking rp54xx servers in deskside enclosures can damage equipment, may cause injury to personnel, and may void your warranty or service contract.

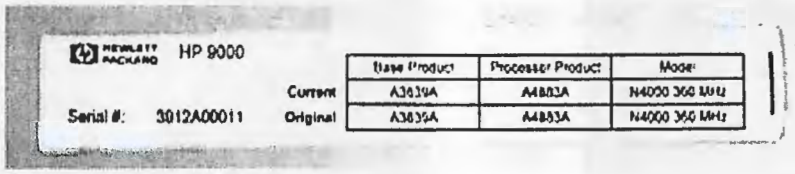
Step 6. Install the Front Bezel.

Step 7. Locate the two pull-tabs. One pull-tab is longer than the other. The shorter pull-tab is blank on both sides. The back of the shorter pull-tab provides a writable surface for Customer use.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
11
1539
Fls: 3701
Doc:

Step 8. Locate the plastic bag containing the label sheet (taped to the server).

Step 9. Remove the label containing serial number, base product, processor product, and model information from the label sheet and apply to the back of the longer pull-tab.



NOTE Pull-tab and label shown above is for an rp74xx server. rp54xx uses the same style label and similar pull-tab.

Step 10. Insert the pull-tabs into the front bezel. Install the longer pull-tab in the left side plastic window in such a way that the rp54xx logo is visible. Install the shorter pull-tab in the right side plastic window with either surface visible. Refer to the diagram above for pull-tab locations.

ECT
CPL 0487 SP - AC

Install Stand-Alone Server in a Cabinet

The following describes how to install the A5556A slide-tray assembly into an approved HP cabinet in preparation for installing an rp54xx server.

This slide-tray assembly can be installed in an HP E-Series cabinet or other HP cabinets approved for rp54xx system installation. To install the A5556A slide-tray assembly in an approved HP equipment cabinet, proceed as follows:

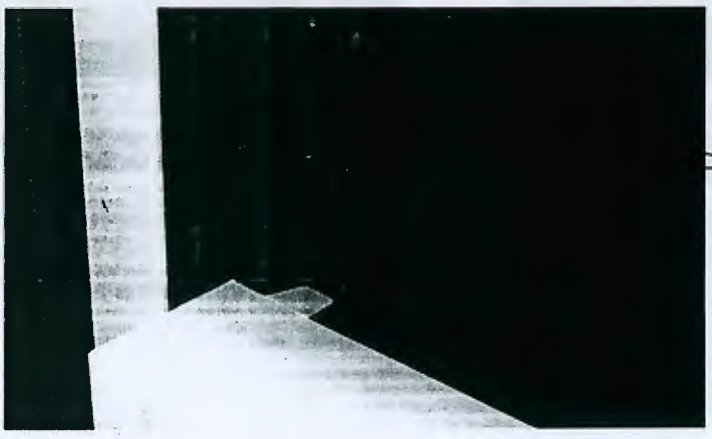
Step 1. Determine what type of cabinet you are installing the slide-tray assembly into.

a. E-Series cabinets have:

- Parchment white, plastic, sectional, side panels
- Black painted vertical frame posts with a partial return flange.

b. Approved, non-E-Series, cabinets have:

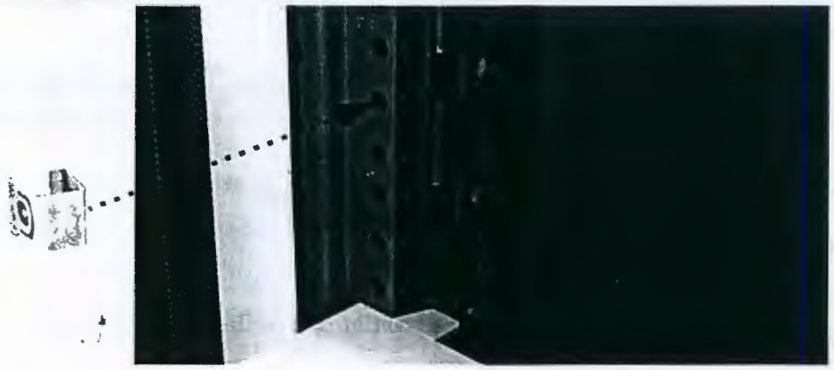
- Single piece metal side panels
- Gray painted verticle frame posts with full return flanges.



Step 2. Note the vertical, rectangular, slots in the return flanges on the vertical mounting posts. Determine into which of these vertical slots the slide/tray kit will be installed. This is done by counting down eight rectangular slots from the top of the cabinet or the bottom of the equipment above.

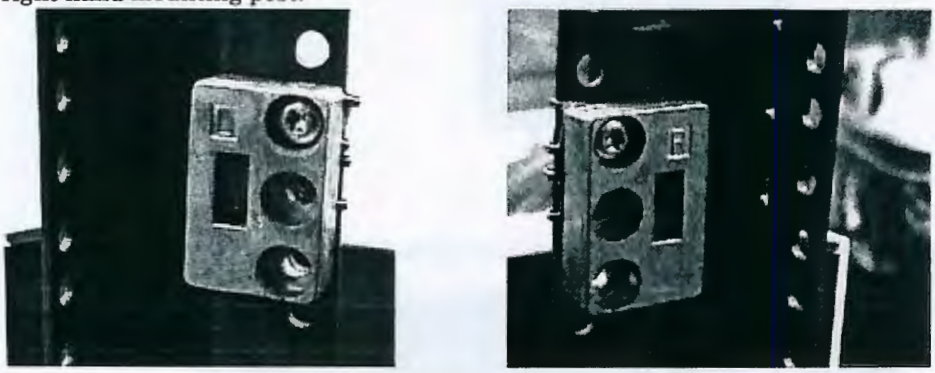
RQS Nº 03/2005 - CN
CPMI - CORREIOS
1540
Fls:
Doc: 3701

Step 3. On the front vertical mounting posts *only*, slide M5 sheet metal nuts onto the posts over the holes immediately adjacent to the vertical slots determined in the previous step. Also place M5 sheet metal nuts on the holes directly above these. Orient the sheet metal nuts so that the threaded portion faces towards the outside of the cabinet. There should now be a total of four (4) sheet metal nuts installed.



Step 4. If the cabinet is a non-E-Series cabinet, discard the left hand and right hand aluminum spacers and two of the M5 x 16 screws with cress-cup washers and proceed to step 12.

Step 5. If the cabinet is an E-Series cabinet, place the hook of the aluminum spacer marked "L" (5183-1864) into the appropriate vertical, rectangular slot on the front, left hand mounting post. The hook points downward. Similarly, place the spacer marked "R" (5183-1863) into the appropriate slot on the right hand mounting post.

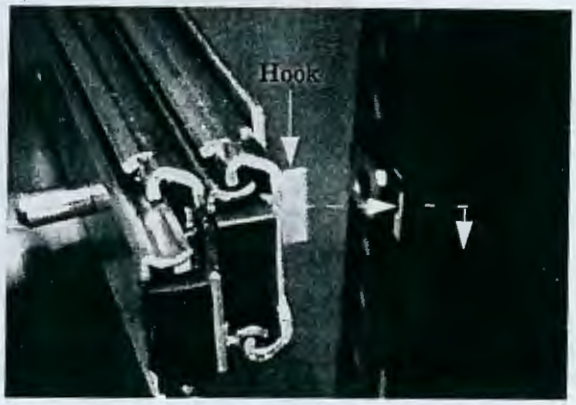


Step 6. Use one M5 x 16 screw with cress-cup washer to attach each spacer to its vertical post. Do this by inserting the screw through the top hole in the spacer, through the mounting rail and tightening it into the sheet metal nut located at that position.

Step 7. Take the left hand slide/bracket assembly (marked 337079-1L) and install it into the left hand vertical mounting posts. This is done by inserting the pin at the rear of the slide's mounting bracket into the 23rd hole in the rear vertical mounting post and inserting the hook at the front of the

F C
24815
Paulo
L - AC

bracket into the vertical, rectangular slot in the aluminum spacer. The slide should be positioned in the cabinet so that it is horizontal and level.



Step 8. Securely fasten the rear of the slide's mounting bracket to the rear vertical mounting post by installing and tightening two of the M5 x 16 screws with cress-cup washers thorough the mounting post, through the slides mounting bracket and into the threaded nuts attached to the mounting bracket.

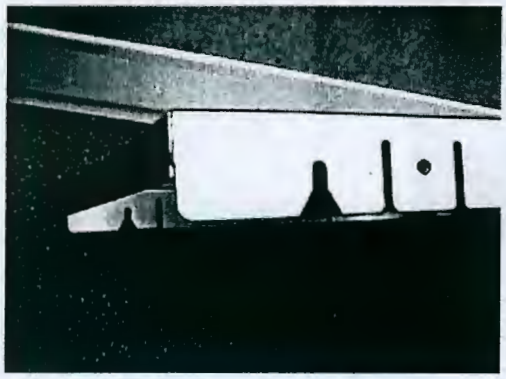
RQS Nº 03/2005 - CN
CPMI - CORREIOS
1541
Fls:
3701
Doc:

Step 9. Fully extend the slide so that it is locked in the fully open position.

Step 10. Use an M5 x 30 screw with a cress cup washer to attach the front of the slide to the vertical mounting post. Insert the screw through the slide, through the center hole of the aluminum spacer, through the vertical mounting post, and tighten into the sheet metal nut located at that position.

Step 11. Use a procedure similar to steps 7 through 10 to install the right hand slide/bracket assembly (marked 337079-1R) and then proceed to step 12.

Step 12. Take the tray and place it onto the pins that extend from the slides' inner members. The slots with wide lead-in guides on the side of the tray fit down onto the slides' pins. The flat part of the tray will be on top, and the mounting holes in the top of the tray will be located to the right of the center of the tray. Slide the tray all the way down on both sides so that the pins reach the top of the slots in the side of the tray.



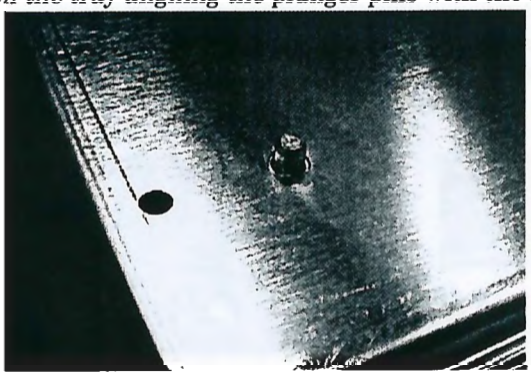
Step 13. Use six, M5 x 12 screws (without washers) to attach the tray to the slides. Three screws are used to attach each slide. Insert the screws through the slides, through the tray and tighten into the threaded nuts located on the inside of the sides of the tray.

3 Pan Head
M5x12 T25 screws
on each side

Step 14. From the bottom of the tray pull the plunger pin down and give it a 1/4 turn to hold it in place.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1542
Fls:
3701
Doc:

Step 15. Position the server on the tray aligning the plunger pins with the alignment holes in the chassis.



Step 16. Release the plunger pins to secure the server.

E C T
CPL - AC
1981
Paula

Stationary L-Bracket Rail Assembly

rp54xx servers may be installed into E-Series and approved Non- E-Series cabinets using stationary L-bracket rail assembly kits listed below.

NOTE rp54xx servers are supported in Hewlett-Packard E-series and approved Non- E-series Hewlett-Packard cabinets, and approved rail kits.

For information on additional qualified 3rd party cabinets and rail kits, contact the nearest Hewlett-Packard Response Center.

Cabinet Type	Rail Kit Product Number
E-Series HP Cabinet	A5575A
Other Approved HP Cabinet	A5562A

Identifying Approved Non-E-Series HP Cabinets

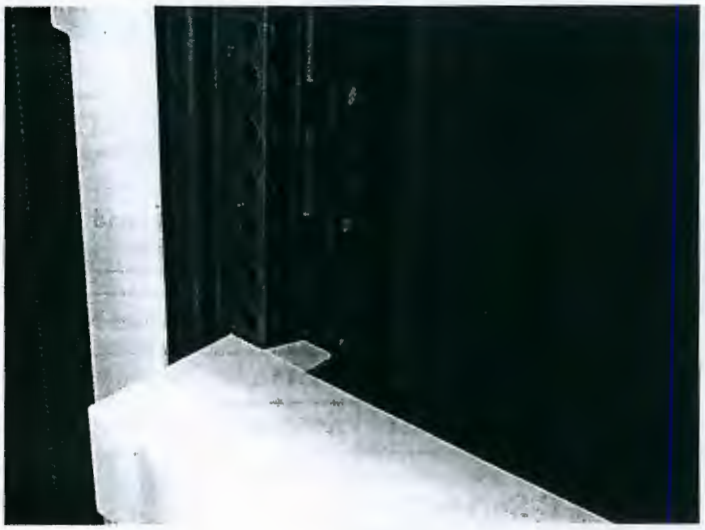
Approved Non- E-Series cabinets have black frames, one piece outside sheet metal skins, a partial return flange, and *requires* the installation of the aluminum spacer blocks, supplied with the rail kits.

Approved Non- E-Series cabinets include the following product numbers: A1883A, A1884A, A1896A, A1897A, C1897A, C2785A, C2786A, and C2787A.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1543
Fls:
Doc: 3701

Identifying E-Series HP Cabinets

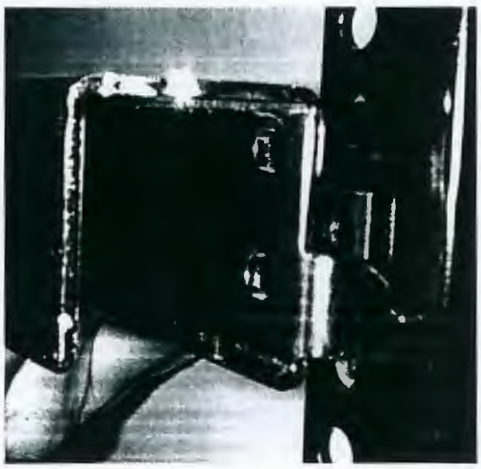
E-Series cabinets have light gray frames, sectioned, plastic outside "skins", a full return flange, and does *not* require the installation of the aluminum spacer block supplied, with the rail kits.



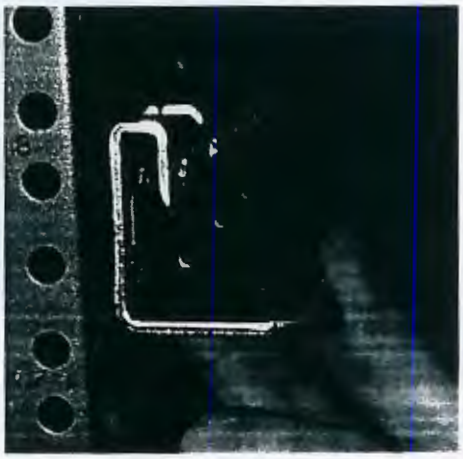
E-Series cabinets include the following product numbers: A5134A, A5136A, A5136A, A4900A, A4901A, A4902A, J1500A, J1502A, and J1502A.

Identifying Static Rail Kit

Hewlett-Packard has currently approved two static rail kits for use in cabinet mounting the rp54xx server. They are illustrated below.



A5562A Kit Rail



A5575A Kit Rail

Installing Stationary Rails

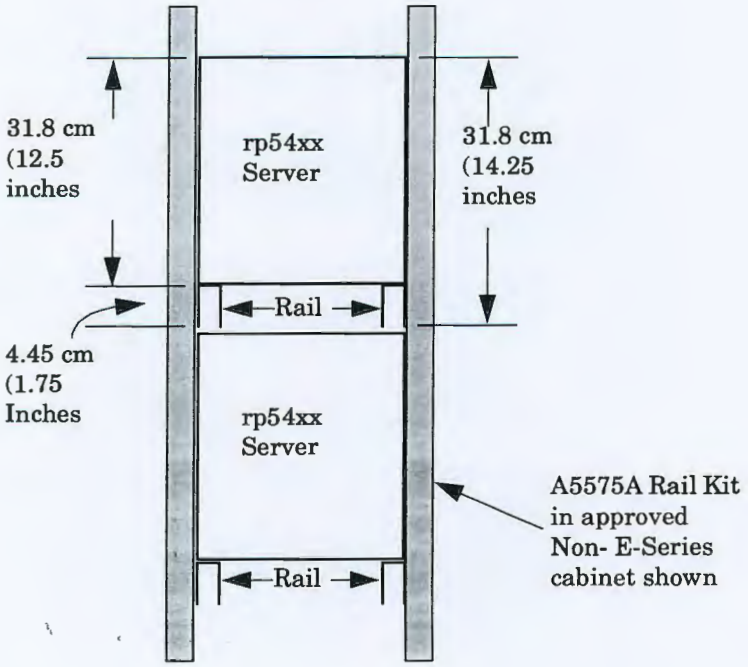
The installation of stationary rails is similar for most cabinet and rail combinations. The key considerations to are:

- Ensure that all safety precautions are read, understood, and observed
- Follow all installation instructions provided with the cabinet and rail kits, and
- Ensure that the rails extend out from the cabinet posts sufficiently to properly and safely support the equipment being installed.

To install an rp54xx server on stationary rails in an approved cabinet proceed as follows:

Step 1. Locate the rail mounting height in the cabinet. Allow for the following space requirements:

- For each rp54xx server, allow 31.8cm (12.5 inches) vertically (7 EIAs or Rack Units (RUs).
- If installing the A5575A rail kit, allow an *additional* vertical 4.45cm (1.75 inches (1 EIA) each set of rails.



Step 2. Install sheet metal nut(s) in the vertical cabinet posts at the required height for the kit being installed:

- Install the first nut either:
  - — 4.45 cm (1.75 Inches) above the top, or
  - — 31.8 cm (12.5 inches) below the bottom of the last server.
- If installing a A5562A rail kit, install the second nut in the next frame hole below the first.

Step 3. Hold the rail in place and insert and tighten the screws.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1544
Fls:
3701
Doc:

For installation of other qualified cabinet and rail combinations refer to the safety precautions and instructions accompanying them.

E C T
4307
Paula
CPL - AC

3 Installing Additional Components

RQS Nº 03/2005 - CN
CPMI - CORREIOS
23
1545
Fls:
3701
Doc:

Additional Components

Some internal components are too delicate to be installed in the server prior to shipping. These internal components are shipped with the server, but are packed separately. They can be installed after the cabinet has been unpacked and positioned.

Some of the internal components that are packed separately are not user-installable. To maintain warranty validation, these items *must* be installed by a Hewlett-Packard Customer Engineer.

If you received either (or both) of the components listed below, contact your Hewlett-Packard provider to arrange for installation.

- Central Processing Units (CPUs)
- Power Distribution Units (PDUs)

Installing Memory

Memory Configuration Rules

rp54xx servers have 16 slots (8 DIMM pairs) for memory DIMMs. These slots are numbered 0a/b, 1a/b,... 7a/b. 8 of these slots (4a/b - 7a/b) are disabled on rp5400 servers. rp5450 servers can access all slots. rp5400 and rp5450 servers have DIMM slots located on the System Board.

rp5470 servers install DIMMs using Memory Carriers. The Memory Carriers fit into slots on the System Board.

The following rules govern the installation of memory DIMMs for rp5400, rp5450, and rp5470 servers:

- Memory must be installed in DIMM pairs.
- The capacity of DIMMs within a pair must be the same.
- Install DIMMs with the greatest capacity in the lowest slot numbers.
- Install DIMMs the following slot order: 0a/b, 1a/b, 2a/b, 3a/b, and so on.

Installing rp5400 and/or rp5450 DIMMs

Step 1. Power down and *unplug* the rp54xx server.

CAUTION DC voltages are present when the server is connected to AC power. Do not install or service rp54xx internal components while DC voltage is present. Failure to observe this precaution can result in damage to the server.

Step 2. Loosen the captive T-15 screws that hold the top cover in place, then grasp the strap handle, raise the cover slightly, and pull the cover toward the front of the server to free the cover tabs from the slots in the chassis. The air baffle will be exposed.

Step 3. Make the top of the server accessible for service.

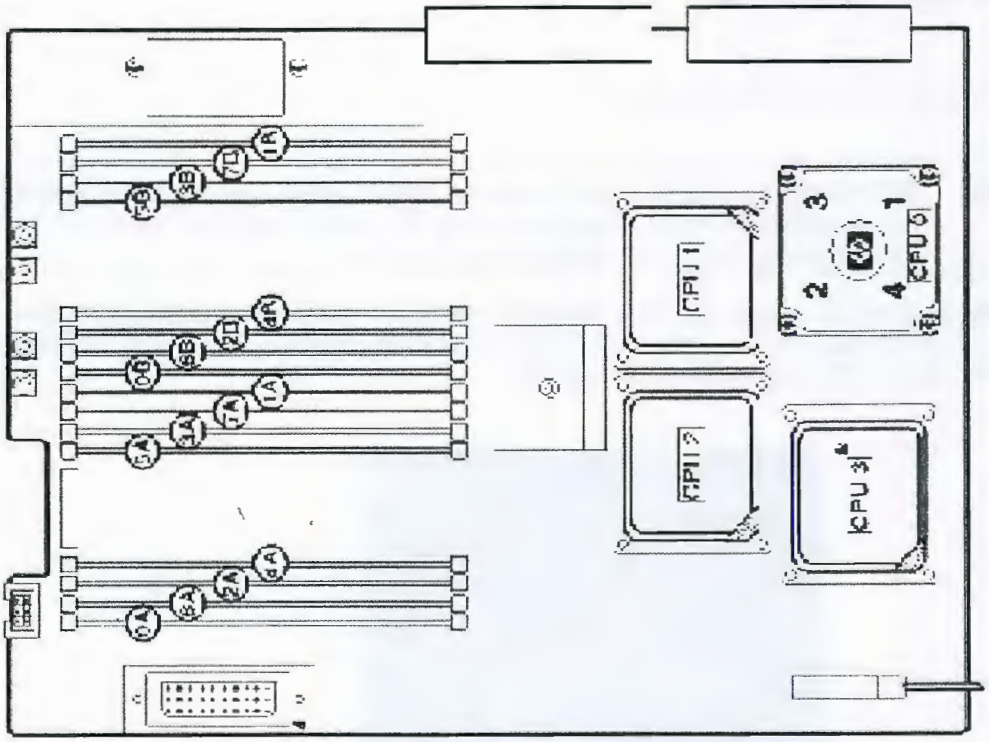
ECT
2805
Paulo
L - AC
ROS Nº 03/2005 - CN
CPMI - CORREIOS
1546
Fls: 3701
Doc:

Step 4. Loosen the captive T-15 screws on the air baffle. Grasp the two handles on the baffle, and lift the baffle remove it.

CAUTION Observe all ElectroStatic Discharge (ESD) precautions Do not touch internal components. Failure to observe ESD precautions can cause damage to components.

Step 5. Observe Electrostatic Discharge (ESD) precautions.

Step 6. Refer to the following graphic for memory slot locations.

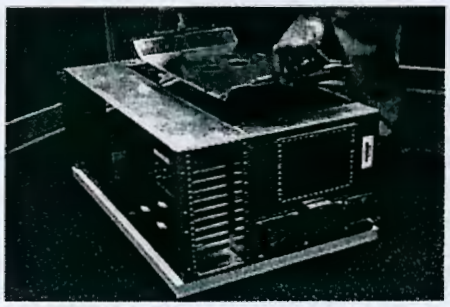


E C T
1803
Paulo
L - AC

Locate the correct DIMM pair slots. Insert the DIMM connectors into the guides until the card snaps firmly in place. It may be necessary to apply downward force using the palm of your hand on the DIMM. Observe the top of the DIMM to make sure one side is not higher than the other.

NOTE It may be necessary to remove PSM 1 when installing a DIMM in slot 0a and PSM 0 when installing a DIMM in slot 1b. If either PSM is removed to install memory, ensure it is re-installed.

Step 7. Replace the air baffle. Tighten the four captive screws to secure the air baffle in place.



Step 8. Replace the top cover. Tighten the four captive screws to secure the top cover in place.

Step 9. For rack configurations, insert the rp54xx server back into the rack.

Step 10. For deskside enclosure configurations, replace the deskside enclosure cover.

Step 11. Power the rp54xx server on.

Step 12. Use the BCH command `in me` to verify the system recognizes the memory that you have just added.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1547
Fls: 3701
Doc:

Installing rp5470 DIMMs

DIMMs for the rp5470 system are installed in memory carriers instead of the system board, as are the other rp54xx systems. However, rp5470 memory carriers are also located on the system board, so the method for opening and closing the system is the same. Procedures for removing and replacing the server top and baffle are listed below, without the pictures shown in the section titled, "*Installing rp5400 and/or rp5450 DIMMs.*" If you wish to reveiw the pictures, please refer to the aforementioned section.

Step 1. Power down and unplug the rp54xx server.

NOTE DC voltages are present when the server is connected to AC power. Do not attempt to install or service: CPUs, Memory, PSMs, the Platform Monitor or PCI I/O cards installed in non-Turbo slots (1-6) while DC voltage is present. Failure to observe this warning may result in damage to the server.

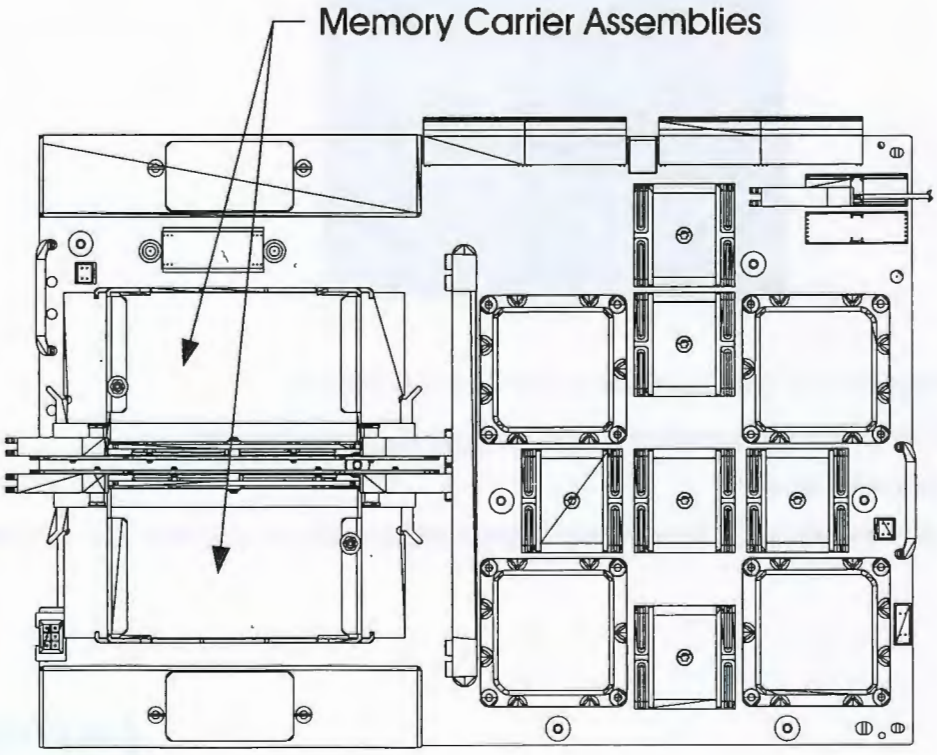
Step 2. Make the top of the server accessible for service.

Step 3. Loosen the captive T-15 screws that hold the top cover in place, then grasp the strap handle, raise the cover slightly, and pull the cover toward the front of the server to free the cover tabs from the slots in the chassis. The air baffle will be exposed.

Step 4. Loosen the four (4) captive T-15 screws on the air baffle. Grasp the two handles on the baffle, and lift and remove the baffle.

Step 5. Observe Electrostatic Discharge (ESD) precautions.

Step 6. Refer to the following graphic for Memory Carrier locations.



a. Locate the Memory Carrier and pull up on the extractor levers on each end of the Memory Carrier to unseat the Memory Carrier from its socket.

b. When the Memory Carrier unseats from the socket, pull it away from the System Board.

c. Loosen the captive screws that secure the DIMM Clip and remove the DIMM Clip from the Memory Carrier.

d. Seat the memory DIMM into its socket on the Memory Carrier.

e. Press the extractor levers on each end of the memory DIMM slot inward until the levers snap into place.

f. Attach the Memory Clip to the Memory Carrier with the DIMM slot markings on the top of the Memory Clip aligned with the DIMM slot markings on the Memory Carrier.

g. Secure the Memory Clip using the captive screws.

h. Seat the Memory Carrier into the appropriate slot on the System Board.

i. Push down on the extractor levers and snap them into place.

Step 7. Replace the air baffle. Tighten the four captive screws to secure the air baffle in place.

Step 8. Replace the top cover. Slide the cover tabs into the slots in the chassis and close the cover. Tighten the two captive screws to secure the top cover in place.

Step 9. For rack configurations, insert the rp54xx server back into the rack.

Step 10. For deskside enclosure configurations, replace the deskside enclosure cover.

Step 11. Power the rp54xx server on.

Step 12. Use the BCH command `in me` to verify the system recognizes the memory that you have just added.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1548
Fls: 29
3701
Doc:

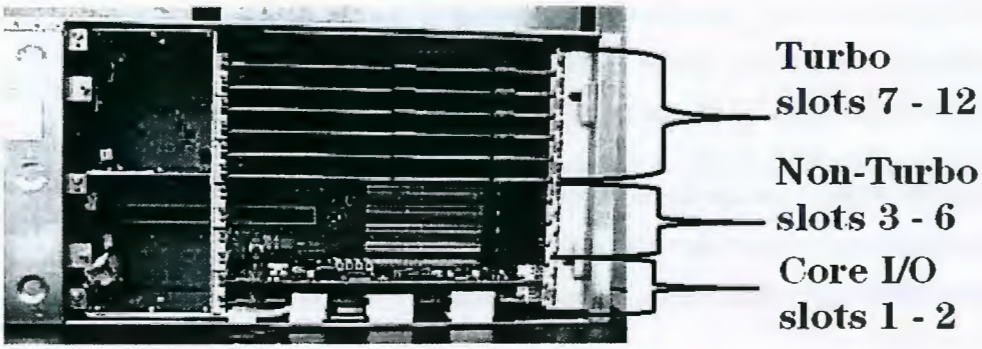
Installing Peripheral Component Interconnect (PCI) Cards

rp54xx servers have a total of 12 PCI I/O slots. Slots 1 and 2 are reserved for the LAN/SCSI and GSP Core I/O cards, leaving 10 PCI I/O slots available for Customer use.

rp5400/rp5450 PCI Card Slots

For rp5400 and rp5450 models, 10 PCI I/O slots consist of Turbo and non-Turbo slots. Server PCI slots are shown below.

rp5400/rp5450 PCI Card Slots



- Slots 1 and 2 are reserved for the rp54xx LAN/SCSI and GSP (Guardian Service Processor) Core I/O cards, respectively. Slots 1 and 2 are non-Turbo slots. Non-Turbo slots share a single 250MB/s PCI bus and are incapable of HotPlug functionality. The server must be turned off prior to removing or installing the LAN/SCSI or GSP cards in these slots.
- Slots 3 - 6 are non-Turbo slots. These four Non-Turbo slots share a single 250MB/s PCI bus, run at 33MHz and support 32 and 64-bit PCI cards. Non-Turbo slots are incapable of HotPlug functionality. The server must be turned off prior to removing or installing PCI cards in these slots.
- Slots 7 - 12 are Turbo slots. Each Turbo slot has a dedicated 250MB/s PCI bus, run at 66MHz and support 32 and 64-bit PCI cards. Turbo slots are HotPlug capable. Below each Turbo slot is a plastic PCI card separator. The PCI card separator has two LEDs and a pull tab on the outer edge. The LED's provide power and status for the slot. The pull tab allows the PCI card to be easily removed.

rp5400 servers have access to slots 1, 2 and 8-12 while rp5450 servers have access to all (1-12) slots.

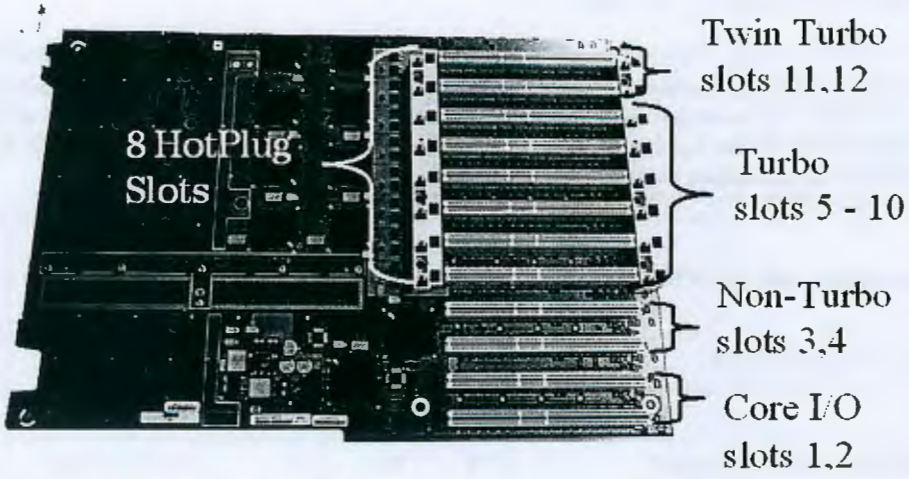
NOTE Slot 3 will become enabled on rp5400 servers with server firmware versions later than 40.48.

A slot 3 enabled label (A5576-84009) is available for rp5400 systems.

F C T
4799
Paula
A C

rp5470 PCI Card Slots

For rp5470 models, the 10 PCI I/O slots consist of Twin Turbo, Turbo, and non-Turbo slots. The following illustration shows the PCI card slot layout.



- Slots 1 and 2 are reserved for the rp54xx LAN/SCSI and GSP (Guardian Service Processor) Core I/O cards, respectively. Slots 1 and 2 are non-Turbo slots. Non-Turbo slots share a single 250MB/s PCI bus and are incapable of HotPlug functionality. The server must be turned off prior to removing or installing the LAN/SCSI or GSP cards in these slots.
- Slots 3 and 4 are non-Turbo slots. These two Non-Turbo slots share a single 250MB/s PCI bus, run at 33MHz and support 32 and 64-bit PCI cards. Non-Turbo slots are incapable of HotPlug functionality. The server must be turned off prior to removing or installing PCI cards in these slots.
- Slots 5 - 10 are Turbo slots. Each Turbo slot has a dedicated 250MB/s PCI bus, run at 66MHz and support 32 and 64-bit PCI cards. Turbo slots are HotPlug capable. Below each Turbo slot is a plastic PCI card separator. The PCI card separator has two LEDs and a pull tab on the outer edge. The LED's provide power and status for the slot. The pull tab allows the PCI card to be easily removed.
- Slots 11 and 12 are Twin Turbo slots. Each Twin Turbo slot has a dedicated 500MB/S PCI bus, runs at 66 MHz, and supports 32- and 64-bit PCI cards. Twin Turbo slots are HotPlug capable. Below each Twin Turbo slot is a plastic PCI card separator. The PCI card separator has two LEDs and a pull tab on the outer edge. The LED's provide power and status for the slot and the pull tab allows the PCI card to be easily removed.

rp5470 servers have access to all (1-12) slots.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1549
Fls:
Doc:

PCI I/O Card Installation Restrictions

Restrictions apply regarding the installation of PCI I/O cards which contain a PCI-to-PCI bridge:

- HP-UX boot is currently not supported for cards that contain a PCI-to-PCI bridge.
- HP-UX patches are required when more than one card containing a PCI-to-PCI bridge is installed in non-Turbo slots.

PCI I/O Card Installation Order

The following table shows a standard factory PCI card installation that begins with slot 12. Use this table as a guideline for installing PCI I/O cards in the field.

NOTE A system shipped from the factory may have a different configuration than the same system built in the field. For example: The factory will install the graphics card in slot 12 and add other cards below. In the field, slot 12 may already be occupied by another PCI card. It is acceptable for the graphics card to be installed in any available Turbo slot.

Product Number	Description (all are PCI cards)	Max	Boot	Load Order *	Part Number	Notes
A6150A	Graphics, Graphics Card	1	No	1	A4982-66501	3,8
A5838A	Combo		No	3	A5838-60001	9
A5483A	ATM 622Mbps MMF Adapter	10	No	4	A5483-60001	10
A4926A	1000Base SX PCI LAN Adapter	10	No	5	A4926-60001	
A4926A	1000Base TX PCI LAN Adapter	10	No	6	A4926-60001	
A6092A	HYPERFabric		No	7	A6092-60001	11
A5158A	FC Taclite		Y	8	A5846-60001	
A5486A	Praesidium Speed Card	10	No	9	A5486-60001	
A5506A	4 Port 100Base TX LAN Adapter	7/10	No	10	A5506-60101	1,2,6
A5506B	4 Port 100Base TX LAN Adapter	7/10	No	10	A5506-60102	
A5150A	Dual Port Ultra 2 SCSI adapter	10	Yes	11	A5150-60001	4
A5149A	Single Port Ultra 2 SCSI HBA	10	Yes	12	A5149-60001	
J3526A	High Perf 4 Ports Synchronous Adapter	10	No	13	5063-1322	7,5
A4800A	FWD SCSI-2 adapter	10	Yes	14	A4800-67002	
A5230A	100Base-T LAN Adapter	10	No	15	B5509-66001	
A3738A	10/100Base-T LAN Adapter	10	No	16	A3738-60001	
A3739A	Dual FDDI LAN Adapter	10	No	17	A3739-60001	
A5783A	Token Ring 4/16/100 Hardware Adapter	10	No	18	A5783-60101	

Product Number	Description (all are PCI cards)	Max	Boot	Load Order *	Part Number	Notes
J3525A	Dual Port Synchronous Adapter	10	No	19	J3525-60001	
J3593A	64 port Serial MUX system card	10	No	20	J3593-60001	
J3592A	8 Port PCI Serial MUX card	4	No	21	J3592-60101	
A6150A	Graphics, USB Card	1	No	22	A6150-60001	
A6150BX	Pinnacle 2 Graphics	1	No	1	A6150-60003	12,13
A6386A	Hyper Fabric 2 Interconnect	10	No	6	A3686-60001	
A5506A	Quad Port 10/100B-TX LAN	10	No	10	A5506-60102	14
A6749A	3.3v 64 Port Terminal MUX	10	No	24	A6749-60001	
A6748A	3.3v 8 Port Terminal MUX	10	No	25	A6748-60001	

*In top down order.

Notes:

1. Card contains a PCI-to-PCI bridge.
2. Requires PHKL_20123, PHKL_20629 and PHNE_19826 or their superseded equivalents.
3. Not supported in non-Turbo slots. Install in Turbo slots only.
4. Requires server firmware revision 39.46 or later.
5. Requires HP-UX 11.1
6. Maximum is 7 for HP-UX versions prior to 11.0. Maximum is 10 for HP-UX version 11.1 and later.
7. Requires PHKL_19543 and PHKL_19544 or their superseded equivalents.
8. Requires HP-UX 11.0 Support Plus (IPR) 0006, June 2000 or later. This product to be released 6/00.
9. Not supported in a shared slot (slots 3-4 for rp5470, slots 3-6 for rp5450, not applicable for rp5400).
10. If you are installing ATM 622 cards in an rp5470 configuration, do not install them in slots 3 and 4 (shared slots).
11. Requires 768 MB for first card and 512 MB for each additional card.
12. Not supported in shared slots.
13. Max of 1. Needs USB card for keyboard and mouse.
14. Contains PCI bridge.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1550
Fls:
3701
Doc:

Installing a PCI Card

Follow these procedures to install a PCI card.

Step 1. Power down and unplug the rp54xx server.

NOTE DC voltages are present when the server is connected to AC power. Do not attempt to install or service: CPUs, Memory, PSMs, the Platform Monitor or PCI I/O cards installed in non-Turbo slots (1-6) while DC voltage is present. Failure to observe this warning may result in damage to the server.

Step 2. Make the right side of the server accessible for service.

Step 3. Using a Torx 15 screwdriver, loosen the captive screws on the right side panel. This panel has a label which shows which PCI I/O slots are available and the corresponding paths. The PCI I/O slot paths for rp5400, rp5450, and rp5470 are shown below.

Slot	rp5400		rp5450		rp5430/rp5470	
	Slot Type	**Path**	**Slot/Type**	**Path**	**Slot Type**	**Path**
12	**Turbo**	**0/4/0**	**Turbo**	**0/4/0**	**Twin Turbo**	**0/10/0**
11	Turbo	0/7/0	Turbo	0/7/0	Twin Turbo	0/12/0
10	Turbo	0/3/0	Turbo	0/3/0	Turbo	0/8/0
9	Turbo	0/6/0	Turbo	0/6/0	Turbo	0/9/0
8	Turbo	0/2/0	Turbo	0/2/0	Turbo	0/3/0
7	Not Available		Turbo	0/5/0	Turbo[a]	0/1/0
6	Not Available		Shared	0/1/0	Turbo[a]	0/5/0
5	Not Available		Shared	0/1/1	Turbo[a]	0/2/0
4	Not Available		Shared	0/1/2	Shared[a]	0/4/0
3	Not Available[b]		Shared	0/1/3	Shared	0/4/2
2	GSP		GSP		GSP	
1	LAN/SCSI		LAN/SCSI		LAN/SCSI	

a. Slot is NOT AVAILABLE for rp5430.
b. Slot 3 becomes available with server firmware versions later than 40.48.

Step 4. Remove the PCI slot cover from the slot that will receive the PCI card. To remove the PCI slot cover, slide the PCI slot cover away from the server.

Front Bezel 123
Memory DIMM 123
PCI I/O Card 124
Power Supply 124
HotSwap Power Converter Fan 124
Platform Monitor 124
Processor Support Module 125
Individual Component Remove/Replace Instructions 126
Extend the Server out the Front 126
Insert the Server from the Front 127
Stand-alone Server Cover Removal 128
Stand-alone Server Cover Replacement 130
Top Cover Removal 131
Top Cover Replacement 132
Side Cover Removal 133
Side Cover Replacement 134
Front Bezel Removal (Single Piece) 135
Front Bezel Replacement (Single Piece) 136
Front Bezel Removal (Two Piece) 137
Front Bezel Replacement (Two Piece) 138
Core I/O Removal 139
Core I/O Replacement 140
PCI Card Separator/Extractor Removal 142
PCI Card Separator/Extractor Replacement 143
HotPlug Disk Drive Removal 144
HotPlug Disk Drive Replacement 149
HotSwap Chassis Fan Cover Removal 152
HotSwap Chassis Fan Cover Replacement 153
HotSwap Chassis Fan Removal 154
HotSwap Chassis Fan Replacement 155
HotSwap Card Cage Fan Removal 156
HotSwap Card Cage Fan Replacement 157
HotSwap Power Supply Removal 158
HotSwap Power Supply Replacement 159
HotSwap Power Converter Fan Removal 160
HotSwap Power Converter Fan Replacement 161
Processor Support Module Removal 162
Processor Support Module Replacement 163
Memory DIMM Removal 164
Memory DIMM Replacement 165
Display Board Removal 166
Display Board Replacement 167
Platform Monitor Removal 168
Platform Monitor Replacement 170
PCI I/O Card Removal 172
PCI I/O Card Replacement 173

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1551
Doc: 3721

Contents

A. Parts and Accessories

CRU Physical Location 176
Customer Replaceable Unit Part Numbers 179

B. System Specifications

Dimensions 182
Uncrating Space 182
Space Requirements 182
Computer Room Physical Space Requirements 183
Computer Room Unpacking Space 184
Electrical 185
Office High Availability Requirements 185
Power Protection 185
Modular PDUs 186
System Power Requirements 186
LAN and Telephone 187
Acoustic Safety Standards 188
Altitude Operation Standards 189
Effects of Altitude 189
Temperature and Humidity Operating Standards 190
Thermal Protection Features 190

C. General Site Preparation Guidelines

Electrical Factors 192
Computer Room Safety 192
Power Consumption 193
Electrical Load Requirements (Circuit Breaker Sizing) 193
Power Quality 193
Distribution Hardware 194
Grounding Systems 195
System Installation Guidelines 197
Environmental Elements 198
Computer Room Preparation 198
Cooling Requirements 198
Humidity Level 200
Dust and Pollution Control 200
Metallic Particulate Contamination 201
Electrostatic Discharge (ESD) Prevention 202
Acoustics 202
Facility Characteristics 203
Floor Loading 203
Windows 205
Space Requirements 206
Delivery Space Requirements 206
Operational Space Requirements 206
Floor Plan Grid 206

Contents

Typical Installation Schedule 201
Site Inspection 208
Delivery Survey 212

ECT CRL - AC 4837 Paula

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1552
Doc: 3781

Tables

Table 6-1. Problem Symptoms and Repair Actions 87
Table 6-2. Chassis Log Error to FRU Decoder 91
Table A-1. Exchange CRUs 179
Table A-2. Non-Exchange CRUs 180
Table B-1. Power Requirements 186
Table C-1. Effect of Humidity on ESD Charge Levels 202
Table C-2. Floor Loading Term Definitions 203
Table C-3. Typical Raised Floor Specifications 204
Table C-4. Customer and Hewlett-Packard Information 208
Table C-5. Site Inspection Checklist 209

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1553
Fls:
3701
Doc:

ECT
CPL - AC
4833
Fls:

Figures

Figure A-1. Server Rear View 176
Figure A-2. Side Service Bay 177
Figure A-3. System Board (Access via Top Service Bay) 177
Figure A-4. Server Front 178
Figure C-1. Raised Floor Metal Strip Ground System 196
Figure C-2. Delivery Survey (Part 1) 213
Figure C-3. Delivery Survey (Part 2) 214

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1554
Fls:
3701
Doc:

E C T
4831
Paula
CPL - AC

Preface

Printing History

The Printing History below identifies the edition dates of this manual. Updates are made to this publication on an unscheduled, *as needed*, basis. The updates will consist of a complete replacement manual and pertinent on-line or CD-ROM documentation.

First Edition ..... November 2002

What's New?

The, *Upgrade Guide, rp5400 Family of Servers*, is new and was developed to provide customers with system maintenance information for those components called customer replaceable units (CRUs). Maintenance of CRUs does not require HP customer engineering services, except when specifically cautioned. The cautions are shown primarily to protect customer product warrantees.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1555
Doc: 3701

ECT
CPL - AC
4829
Paula

1 Server Overview

The rp5400 family of servers are 1-way to 4-way servers based on the PA-RISC processor architecture. The rp5400 family of servers accommodate up to 16GB of memory and internal peripherals including disks and DVD ROM/Tape. High availability features include HotSwap fans and power supplies, and HotPlug internal disk drives. The supported operating system is HP-UX.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1556
Doc: 3701

E C T
4827
Paula
C P L - AC

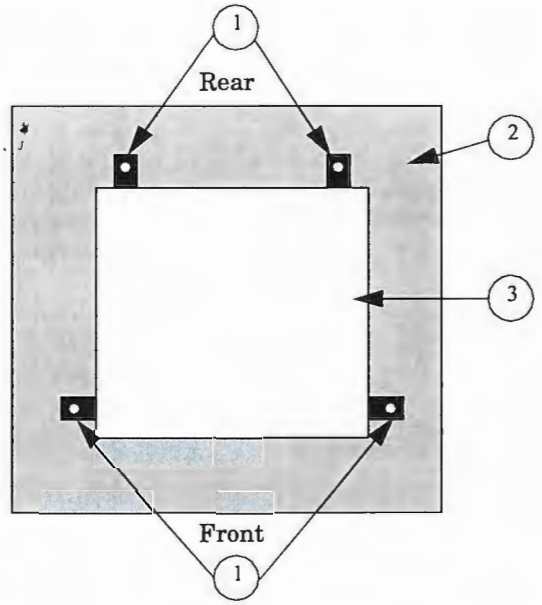
2 Server Unpacking and Installation

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1557
3701
Doc: 3

Factory Integrated rp54xx Cabinet Installation

A factory integrated server is one in which the rp54xx server and associated components are pre-assembled and shipped from the factory already installed in a Hewlett-Packard E-Series cabinet. Factory integrated systems reduce the amount of time required to set-up and begin server operation.

1. Carefully remove the carton and anti-static bag from the pallet.
2. Remove the front two (2) L-brackets. Retain the 1/2-inch bolts for later use.



1. Shipping L-Bracket
2. Shipping Pallet
3. Cabinet (Top View)

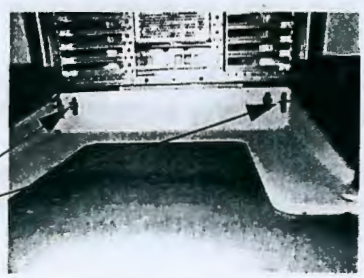
NOTE As viewed from the front, one bracket is located on each side at the base of the cabinet near the front.

E C T
3.4825
Paula
L - AC I

3. At the rear of the cabinet:

   a. Open the door.

   b. Remove the anti-tip foot by removing and retaining the two (2) 1/2-inch bolts.



For Shipping: L-brackets are mounted behind anti-tip foot. Same bolts secure both.

   c. Remove the two (2) L-brackets (revealed by removing the anti-tip foot).

4. Remove the two ramps from the pallet and carefully place them into the slots at the front of the pallet.

WARNING **Use extreme care when rolling the racked system down the ramps. A rack containing one rp54xx can weigh up to 418 lbs. Do not stand in front of the ramps when rolling the cabinet off the pallet or injury may occur. All but the smallest configurations require two persons to safely remove the rack from the pallet.**

If anti-tip feet or ballast are not installed or are improperly installed the cabinet can tip. Failure to follow this precaution can cause injury to personnel or damage to equipment.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1558
Doc: 3701

5. Straighten the rollers on the cabinet base, if needed, and carefully roll it down the ramps.

WARNING ***After removing the server from the pallet, Do not move the cabinet unless the anti-tip feet are installed!*** **The cabinet can tip if care is not used. Due to their low ground clearance the feet may catch on irregularities on the floor, thresholds, or ramps.**

Do not move the cabinet without first installing the anti-tip feet. **The cabinet may tip if moved without the anti-tip feet or ballast installed.**

Do not move the cabinet after installing the anti-tip feet unless they are in the fully-raised position. **Once installed, the anti-tip feet must be fully raised to allow ground clearance.**

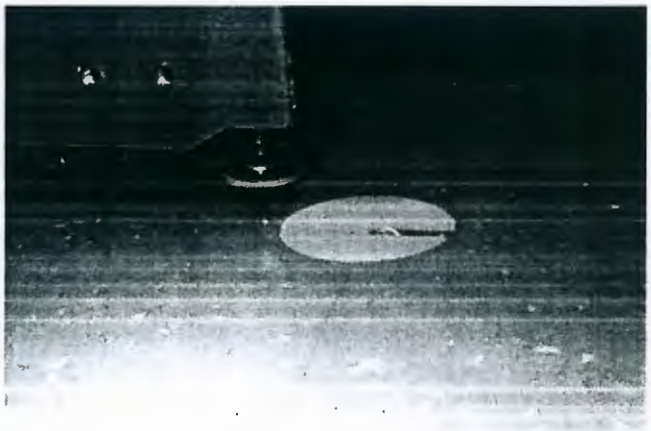
Because of their low ground clearance, the fully-raised anti-tip feet may need to be removed *temporarily* to clear some obstacles such as door jambs, ramps, and other large irregularities or obstructions on the floor.

If you must temporarily remove the anti-tip feet to clear an obstacle, use extreme caution when moving the cabinet. Always reinstall the anti-tip feet as soon as the obstacle has been cleared.

Lower and secure both the anti-tip feet and the cabinet leveling/stabilizer feet once the cabinet is in place.

Failure to follow these precautions can result in equipment damage or personal injury.

6. Install the front and rear anti-tip feet using the 1/2 inch bolts provided. Ensure that the anti-tip feet are installed in the fully up position in the mounting slots. This will provide maximum ground clearance while moving the cabinet to its final position.
7. Carefully move the cabinet to its installation location.
8. Lower the anti-tip feet to the fully down position and adjust the cabinet leveling feet for best cabinet stability.



E C T
4823
Paula
CPL - AC

Receive and Unpack A Non-Integrated Server

WARNING **The typical rp54xx system can weigh up to 68kg (150lbs). *HP recommends using an an approved lifting device*. Lift and move the server in accordance with all local safety regulations. Failure to follow this precaution can cause injury to personnel or damage to equipment.**

Unpacking the server

The following procedure describes the steps involved in unpacking the server, whether to function as a stand-alone Deskside unit, or to be integrated into a cabinet.

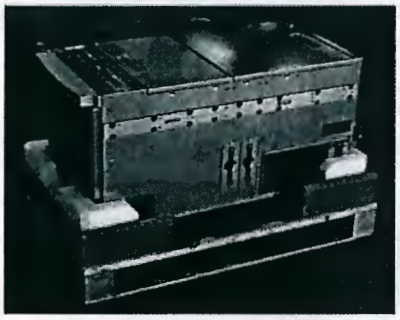
Step 1. Remove the shipping carton and anti-static bag from the server as depicted below.

ROS Nº 03/2005 - CN
CPMI - CORREIOS
1559
Fls:
3701
Doc:

NOTE The packaging for rp74xx and rp54xx servers is the same, rp74xx is shown.

Step 2. If you are moving the server manually, use three people to lift the server from the packing material and pallet. Carefully move the server to the selected location.

Step 3. If you are moving the server by an approved lifting device (such as Genie Lift ™), remove the tear flap from the front lip of the carton bottom to allow access to the server, as illustrated below. Removal of the tear flap will reveal a slot between the bottom of the server and the inside bottom of the cardboard box.



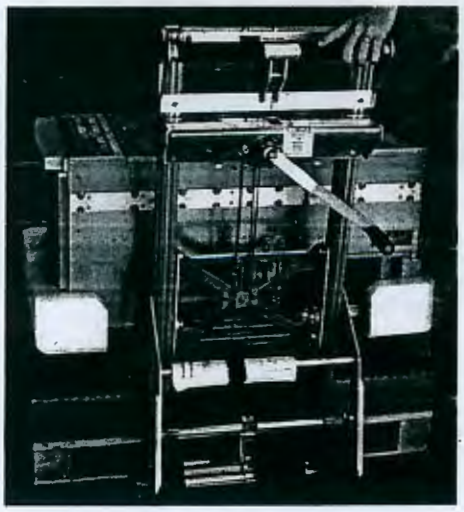
ECT
CPL - AC

Step 4. Carefully raise the lift's platform so that it will slide into the slot located ***under*** the center of the server, but ***over*** the top of the pallet.

Lifting Device Platform.

NOTE The server's center of gravity will vary with the hardware configuration, but it is generally located slightly behind the middle of the server.

Step 5. Raise the lifting device platform enough for the server to clear the pallet and packing materials, as show below.



RQS Nº 03/2005 - CN
CPMI - CORREIOS
1560
Fls: 3701
Doc:

Install Deskside Server

The following section describes the installation of a server into a Deskside enclosure for installation in an office environment.

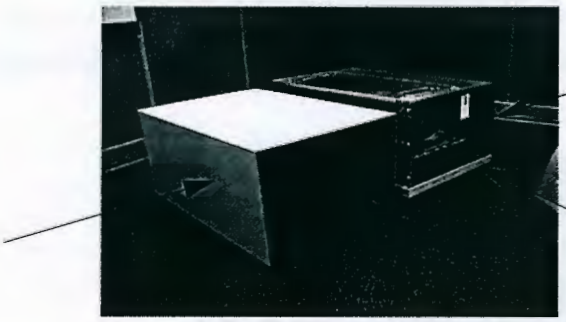
WARNING **The typical rp54xx system can weigh up to 68kg (150lbs). *HP recommends using an approved lifting device.***

- **Lift and move the server in accordance with all local safety regulations.**
- **Do not attempt to lift the server by the plastic handles on the top and side covers.**

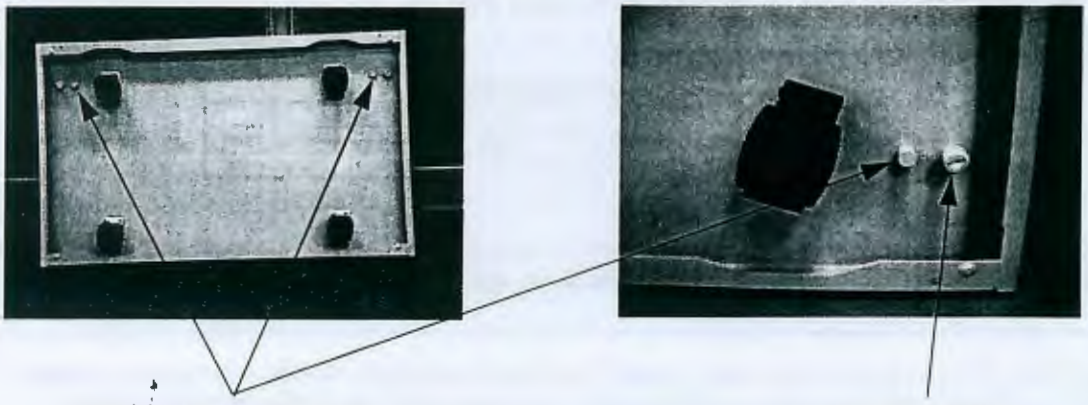
Failure to follow these precautions can cause injury to personnel or damage to equipment.

Step 1. Unpack the server.

Step 2. Unpack the deskside enclosure.



NOTE Ensure that the positioning spring pins in the enclosure base align with the alignment holes in the bottom of the server.



Step 3. Position the server on the wheeled enclosure base.

Step 4. Tighten the two captive screws in the enclosure base to secure the server to the base.

Step 5. Position the enclosure cover (outside skin) over the server and install and tighten the screws to secure it to the base.

NOTE The perforations and the lip of the outside skin should be toward the rear of the server.

WARNING **Stacking rp54xx servers in deskside enclosures is *not* supported.**

Stacking rp54xx servers in deskside enclosures can damage equipment, may cause injury to personnel, and may void your warranty or service contract.

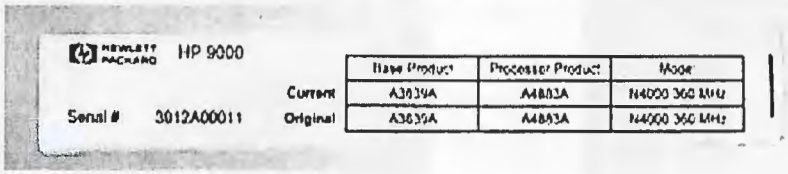
Step 6. Install the Front Bezel.

Step 7. Locate the two pull-tabs. One pull-tab is longer than the other. The shorter pull-tab is blank on both sides. The back of the shorter pull-tab provides a writable surface for Customer use.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1561
Doc: 3701

Step 8. Locate the plastic bag containing the label sheet (taped to the server).

Step 9. Remove the label containing serial number, base product, processor product, and model information from the label sheet and apply to the back of the longer pull-tab.



NOTE Pull-tab and label shown above is for an rp74xx server. rp54xx uses the same style label and similar pull-tab.

Step 10. Insert the pull-tabs into the front bezel. Install the longer pull-tab in the left side plastic window in such a way that the rp54xx logo is visible. Install the shorter pull-tab in the right side plastic window with either surface visible. Refer to the diagram above for pull-tab locations.

E C T
CPL - AC

Install Stand-Alone Server in a Cabinet

The following describes how to install the A5556A slide-tray assembly into an approved HP cabinet in preparation for installing an rp54xx server.

This slide-tray assembly can be installed in an HP E-Series cabinet or other HP cabinets approved for rp54xx system installation. To install the A5556A slide-tray assembly in an approved HP equipment cabinet, proceed as follows:

Step 1. Determine what type of cabinet you are installing the slide-tray assembly into.

a. E-Series cabinets have:

- Parchment white, plastic, sectional, side panels
- Black painted vertical frame posts with a partial return flange.

Vertical,
Rectangular,
Mounting Slots

b. Approved, non-E-Series, cabinets have:

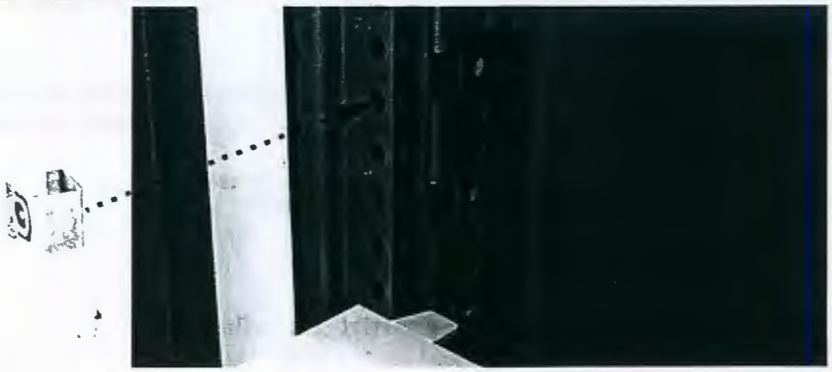
- Single piece metal side panels
- Gray painted verticle frame posts with full return flanges.

Vertical,
Rectangular,
Mounting Slots

Step 2. Note the vertical, rectangular, slots in the return flanges on the vertical mounting posts. Determine into which of these vertical slots the slide/tray kit will be installed. This is done by counting down eight rectangular slots from the top of the cabinet or the bottom of the equipment above.

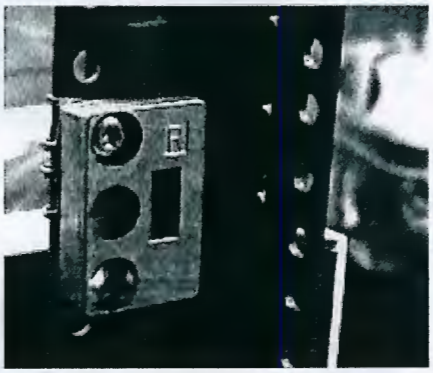
RQS Nº 03/2005 - CN
CPMI - CORREIOS
1562
Fls:
3701
Doc:

Step 3. On the front vertical mounting posts *only*, slide M5 sheet metal nuts onto the posts over the holes immediately adjacent to the vertical slots determined in the previous step. Also place M5 sheet metal nuts on the holes directly above these. Orient the sheet metal nuts so that the threaded portion faces towards the outside of the cabinet. There should now be a total of four (4) sheet metal nuts installed.



Step 4. If the cabinet is a non-E-Series cabinet, discard the left hand and right hand aluminum spacers and two of the M5 x 16 screws with cress-cup washers and proceed to step 12.

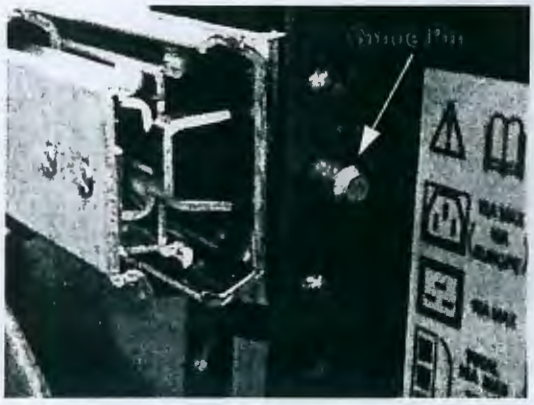
Step 5. If the cabinet is an E-Series cabinet, place the hook of the aluminum spacer marked "L" (5183-1864) into the appropriate vertical, rectangular slot on the front, left hand mounting post. The hook points downward. Similarly, place the spacer marked "R" (5183-1863) into the appropriate slot on the right hand mounting post.

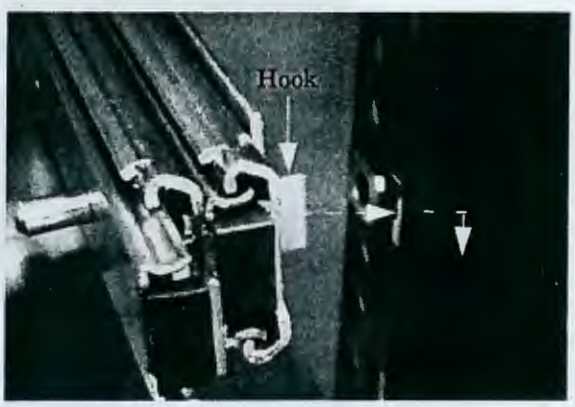


Step 6. Use one M5 x 16 screw with cress-cup washer to attach each spacer to its vertical post. Do this by inserting the screw through the top hole in the spacer, through the mounting rail and tightening it into the sheet metal nut located at that position.

Step 7. Take the left hand slide/bracket assembly (marked 337079-1L) and install it into the left hand vertical mounting posts. This is done by inserting the pin at the rear of the slide's mounting bracket into the 23rd hole in the rear vertical mounting post and inserting the hook at the front of the

bracket into the vertical, rectangular slot in the aluminum spacer. The slide should be positioned in the cabinet so that it is horizontal and level.





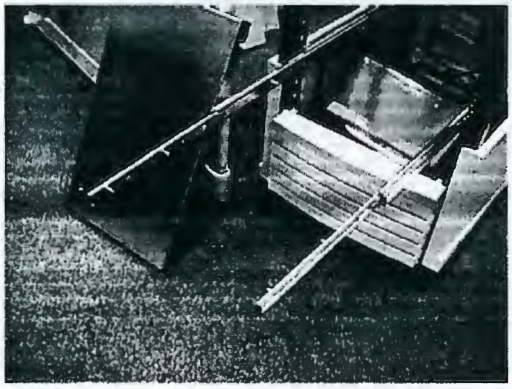
Step 8. Securely fasten the rear of the slide's mounting bracket to the rear vertical mounting post by installing and tightening two of the M5 x 16 screws with cress-cup washers thorough the mounting post, through the slides mounting bracket and into the threaded nuts attached to the mounting bracket.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1563
Fls:
3701
Doc:

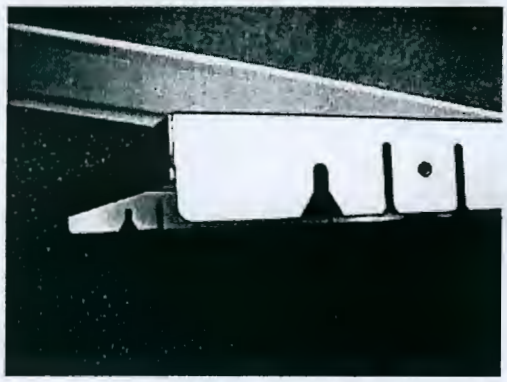
Step 9. Fully extend the slide so that it is locked in the fully open position.

Step 10. Use an M5 x 30 screw with a cress cup washer to attach the front of the slide to the vertical mounting post. Insert the screw through the slide, through the center hole of the aluminum spacer, through the vertical mounting post, and tighten into the sheet metal nut located at that position.

Step 11. Use a procedure similar to steps 7 through 10 to install the right hand slide/bracket assembly (marked 337079-1R) and then proceed to step 12.



Step 12. Take the tray and place it onto the pins that extend from the slides' inner members. The slots with wide lead-in guides on the side of the tray fit down onto the slides' pins. The flat part of the tray will be on top, and the mounting holes in the top of the tray will be located to the right of the center of the tray. Slide the tray all the way down on both sides so that the pins reach the top of the slots in the side of the tray.



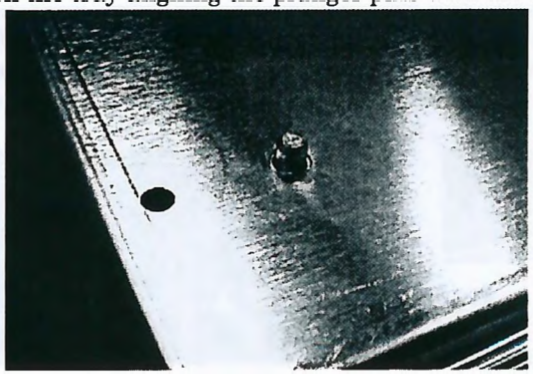
Step 13. Use six, M5 x 12 screws (without washers) to attach the tray to the slides. Three screws are used to attach each slide. Insert the screws through the slides, through the tray and tighten into the threaded nuts located on the inside of the sides of the tray.

3 Pan Head
M5x12 T25 screws
on each side

Step 14. From the bottom of the tray pull the plunger pin down and give it a 1/4 turn to hold it in place.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1564
Fls:
3701
Doc:

Step 15. Position the server on the tray aligning the plunger pins with the alignment holes in the chassis.



Step 16. Release the plunger pins to secure the server.

E C T
CPL - AC
48K Paula

Stationary L-Bracket Rail Assembly

rp54xx servers may be installed into E-Series and approved Non- E-Series cabinets using stationary L-bracket rail assembly kits listed below.

NOTE rp54xx servers are supported in Hewlett-Packard E-series and approved Non- E-series Hewlett-Packard cabinets, and approved rail kits.

For information on additional qualified 3rd party cabinets and rail kits, contact the nearest Hewlett-Packard Response Center.

Cabinet Type	Rail Kit Product Number
E-Series HP Cabinet	A5575A
Other Approved HP Cabinet	A5562A

Identifying Approved Non-E-Series HP Cabinets

Approved Non- E-Series cabinets have black frames, one piece outside sheet metal skins, a partial return flange, and *requires* the installation of the aluminum spacer blocks, supplied with the rail kits.

Approved Non- E-Series cabinets include the following product numbers: A1883A, A1884A, A1896A, A1897A, C1897A, C2785A, C2786A, and C2787A.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1565
Fls: 3701
Doc:

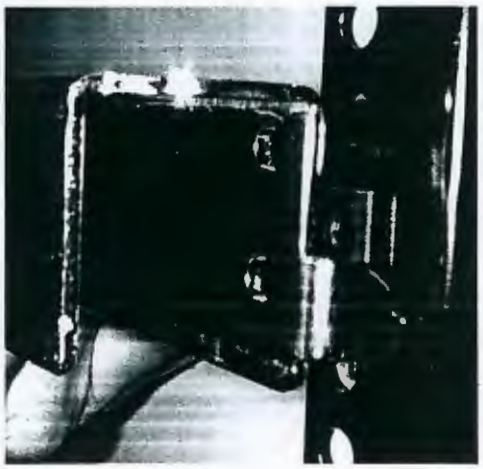
Identifying E-Series HP Cabinets

E-Series cabinets have light gray frames, sectioned, plastic outside "skins", a full return flange, and does *not* require the installation of the aluminum spacer block supplied, with the rail kits.

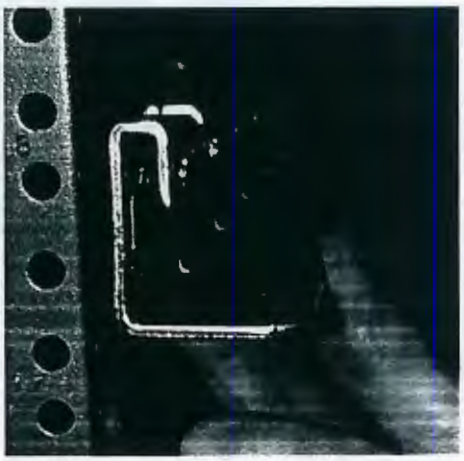
E-Series cabinets include the following product numbers: A5134A, A5136A, A5136A, A4900A, A4901A, A4902A, J1500A, J1502A, and J1502A.

Identifying Static Rail Kit

Hewlett-Packard has currently approved two static rail kits for use in cabinet mounting the rp54xx server. They are illustrated below.



A5562A Kit Rail



A5575A Kit Rail

Installing Stationary Rails

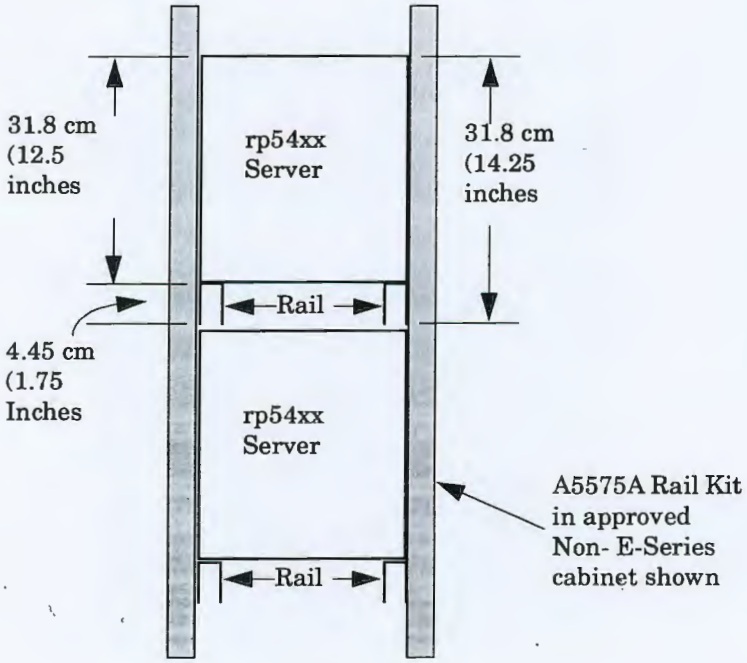
The installation of stationary rails is similar for most cabinet and rail combinations. The key considerations to are:

- Ensure that all safety precautions are read, understood, and observed
- Follow all installation instructions provided with the cabinet and rail kits, and
- Ensure that the rails extend out from the cabinet posts sufficiently to properly and safely support the equipment being installed.

To install an rp54xx server on stationary rails in an approved cabinet proceed as follows:

Step 1. Locate the rail mounting height in the cabinet. Allow for the following space requirements:

- For each rp54xx server, allow 31.8cm (12.5 inches) vertically (7 EIAs or Rack Units (RUs).
- If installing the A5575A rail kit, allow an *additional* vertical 4.45cm (1.75 inches (1 EIA) each set of rails.



Step 2. Install sheet metal nut(s) in the vertical cabinet posts at the required height for the kit being installed:

- Install the first nut either:
  - — 4.45 cm (1.75 Inches) above the top, or
  - — 31.8 cm (12.5 inches) below the bottom of the last server.
- If installing a A5562A rail kit, install the second nut in the next frame hole below the first.

Step 3. Hold the rail in place and insert and tighten the screws.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1566
Fls:
Doc: 3701

For installation of other qualified cabinet and rail combinations refer to the safety precautions and instructions accompanying them.

E C T
4307
Fls.
CPL - AC

3 Installing Additional Components

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1567
Fls:
Doc: 3701

Additional Components

Some internal components are too delicate to be installed in the server prior to shipping. These internal components are shipped with the server, but are packed separately. They can be installed after the cabinet has been unpacked and positioned.

Some of the internal components that are packed separately are not user-installable. To maintain warranty validation, these items *must* be installed by a Hewlett-Packard Customer Engineer.

If you received either (or both) of the components listed below, contact your Hewlett-Packard provider to arrange for installation.

- Central Processing Units (CPUs)
- Power Distribution Units (PDUs)

E C T
24805
Paulo
C A L - A C

Installing Memory

Memory Configuration Rules

rp54xx servers have 16 slots (8 DIMM pairs) for memory DIMMs. These slots are numbered 0a/b, 1a/b,... 7a/b. 8 of these slots (4a/b - 7a/b) are disabled on rp5400 servers. rp5450 servers can access all slots. rp5400 and rp5450 servers have DIMM slots located on the System Board.

rp5470 servers install DIMMs using Memory Carriers. The Memory Carriers fit into slots on the System Board.

The following rules govern the installation of memory DIMMs for rp5400, rp5450, and rp5470 servers:

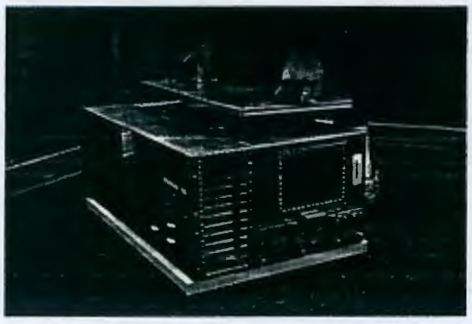
- Memory must be installed in DIMM pairs.
- The capacity of DIMMs within a pair must be the same.
- Install DIMMs with the greatest capacity in the lowest slot numbers.
- Install DIMMs the following slot order: 0a/b, 1a/b, 2a/b, 3a/b, and so on.

Installing rp5400 and/or rp5450 DIMMs

Step 1. Power down and *unplug* the rp54xx server.

CAUTION DC voltages are present when the server is connected to AC power. Do not install or service rp54xx internal components while DC voltage is present. Failure to observe this precaution can result in damage to the server.

Step 2. Loosen the captive T-15 screws that hold the top cover in place, then grasp the strap handle, raise the cover slightly, and pull the cover toward the front of the server to free the cover tabs from the slots in the chassis. The air baffle will be exposed.



Step 3. Make the top of the server accessible for service.

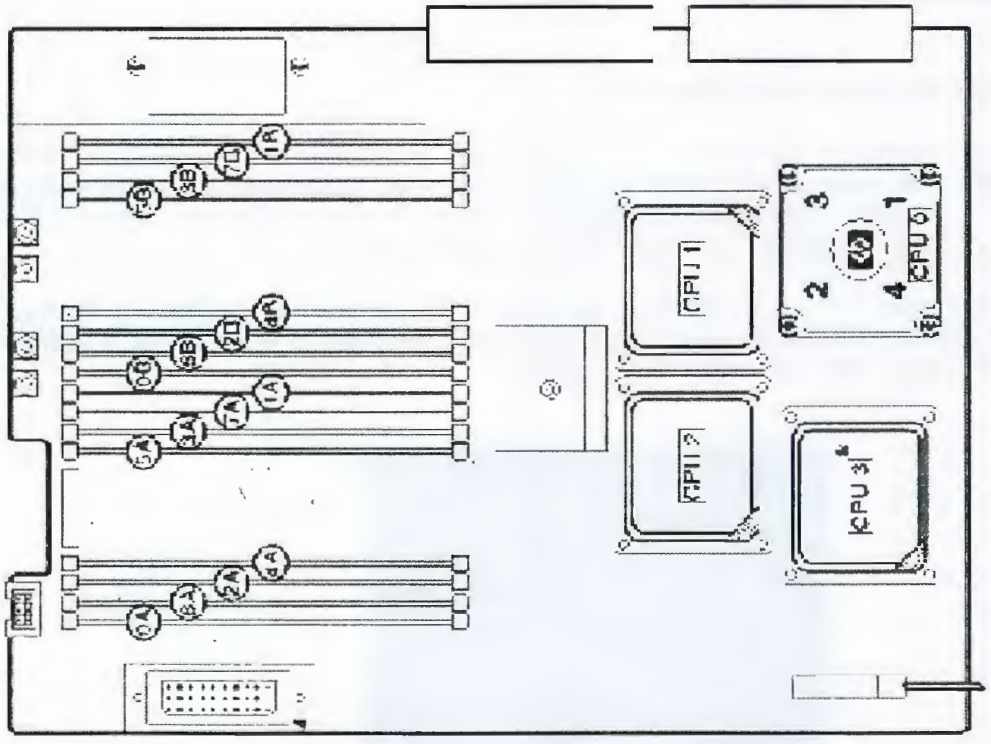
ROS Nº 03/2005 - CN
CPMI - CORREIOS
25
1568
Fls:
3701
Doc:

Step 4. Loosen the captive T-15 screws on the air baffle. Grasp the two handles on the baffle, and lift the baffle remove it.

CAUTION Observe all ElectroStatic Discharge (ESD) precautions Do not touch internal components. Failure to observe ESD precautions can cause damage to components.

Step 5. Observe Electrostatic Discharge (ESD) precautions.

Step 6. Refer to the following graphic for memory slot locations.



Locate the correct DIMM pair slots. Insert the DIMM connectors into the guides until the card snaps firmly in place. It may be necessary to apply downward force using the palm of your hand on the DIMM. Observe the top of the DIMM to make sure one side is not higher than the other.

NOTE It may be necessary to remove PSM 1 when installing a DIMM in slot 0a and PSM 0 when installing a DIMM in slot 1b. If either PSM is removed to install memory, ensure it is re-installed.

Step 7. Replace the air baffle. Tighten the four captive screws to secure the air baffle in place.

Step 8. Replace the top cover. Tighten the four captive screws to secure the top cover in place.

Step 9. For rack configurations, insert the rp54xx server back into the rack.

Step 10. For deskside enclosure configurations, replace the deskside enclosure cover.

Step 11. Power the rp54xx server on.

Step 12. Use the BCH command `in me` to verify the system recognizes the memory that you have just added.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1569
Fls:
3701
Doc:

Installing rp5470 DIMMs

DIMMs for the rp5470 system are installed in memory carriers instead of the system board, as are the other rp54xx systems. However, rp5470 memory carriers are also located on the system board, so the method for opening and closing the system is the same. Procedures for removing and replacing the server top and baffle are listed below, without the pictures shown in the section titled, *"Installing rp5400 and/or rp5450 DIMMs."* If you wish to reveiw the pictures, please refer to the aforementioned section.

Step 1. Power down and unplug the rp54xx server.

NOTE DC voltages are present when the server is connected to AC power. Do not attempt to install or service: CPUs, Memory, PSMs, the Platform Monitor or PCI I/O cards installed in non-Turbo slots (1-6) while DC voltage is present. Failure to observe this warning may result in damage to the server.

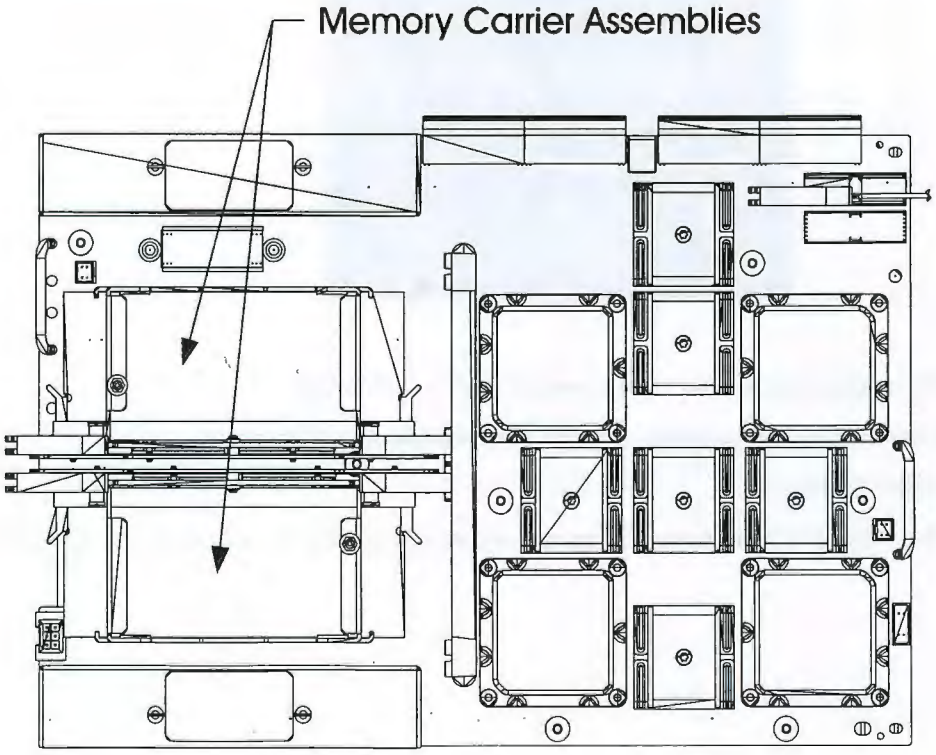
Step 2. Make the top of the server accessible for service.

Step 3. Loosen the captive T-15 screws that hold the top cover in place, then grasp the strap handle, raise the cover slightly, and pull the cover toward the front of the server to free the cover tabs from the slots in the chassis. The air baffle will be exposed.

Step 4. Loosen the four (4) captive T-15 screws on the air baffle. Grasp the two handles on the baffle, and lift and remove the baffle.

Step 5. Observe Electrostatic Discharge (ESD) precautions.

Step 6. Refer to the following graphic for Memory Carrier locations.



a. Locate the Memory Carrier and pull up on the extractor levers on each end of the Memory Carrier to unseat the Memory Carrier from its socket.

b. When the Memory Carrier unseats from the socket, pull it away from the System Board.

c. Loosen the captive screws that secure the DIMM Clip and remove the DIMM Clip from the Memory Carrier.

d. Seat the memory DIMM into its socket on the Memory Carrier.

e. Press the extractor levers on each end of the memory DIMM slot inward until the levers snap into place.

f. Attach the Memory Clip to the Memory Carrier with the DIMM slot markings on the top of the Memory Clip aligned with the DIMM slot markings on the Memory Carrier.

g. Secure the Memory Clip using the captive screws.

h. Seat the Memory Carrier into the appropriate slot on the System Board.

i. Push down on the extractor levers and snap them into place.

Step 7. Replace the air baffle. Tighten the four captive screws to secure the air baffle in place.

Step 8. Replace the top cover. Slide the cover tabs into the slots in the chassis and close the cover. Tighten the two captive screws to secure the top cover in place.

Step 9. For rack configurations, insert the rp54xx server back into the rack.

Step 10. For deskside enclosure configurations, replace the deskside enclosure cover.

Step 11. Power the rp54xx server on.

Step 12. Use the BCH command `in me` to verify the system recognizes the memory that you have just added.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1570
Fls: 3701
Doc:

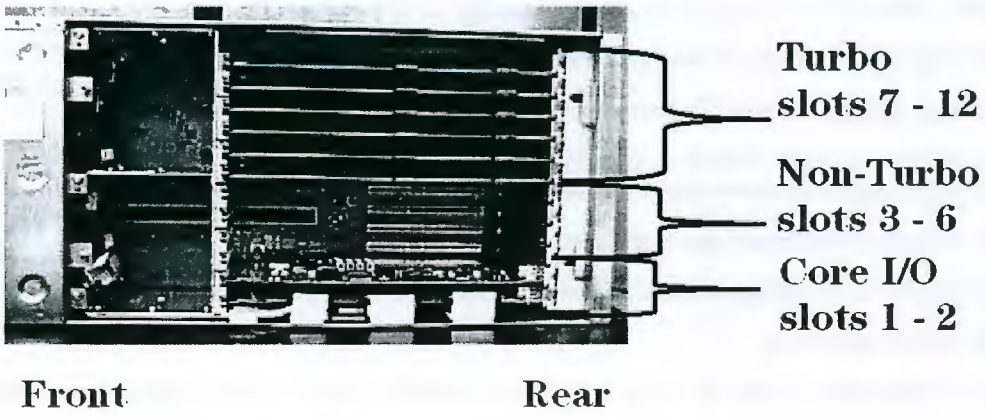
Installing Peripheral Component Interconnect (PCI) Cards

rp54xx servers have a total of 12 PCI I/O slots. Slots 1 and 2 are reserved for the LAN/SCSI and GSP Core I/O cards, leaving 10 PCI I/O slots available for Customer use.

rp5400/rp5450 PCI Card Slots

For rp5400 and rp5450 models, 10 PCI I/O slots consist of Turbo and non-Turbo slots. Server PCI slots are shown below.

rp5400/rp5450 PCI Card Slots



- Slots 1 and 2 are reserved for the rp54xx LAN/SCSI and GSP (Guardian Service Processor) Core I/O cards, respectively. Slots 1 and 2 are non-Turbo slots. Non-Turbo slots share a single 250MB/s PCI bus and are incapable of HotPlug functionality. The server must be turned off prior to removing or installing the LAN/SCSI or GSP cards in these slots.
- Slots 3 - 6 are non-Turbo slots. These four Non-Turbo slots share a single 250MB/s PCI bus, run at 33MHz and support 32 and 64-bit PCI cards. Non-Turbo slots are incapable of HotPlug functionality. The server must be turned off prior to removing or installing PCI cards in these slots.
- Slots 7 - 12 are Turbo slots. Each Turbo slot has a dedicated 250MB/s PCI bus, run at 66MHz and support 32 and 64-bit PCI cards. Turbo slots are HotPlug capable. Below each Turbo slot is a plastic PCI card separator. The PCI card separator has two LEDs and a pull tab on the outer edge. The LED's provide power and status for the slot. The pull tab allows the PCI card to be easily removed.

rp5400 servers have access to slots 1, 2 and 8-12 while rp5450 servers have access to all (1-12) slots.

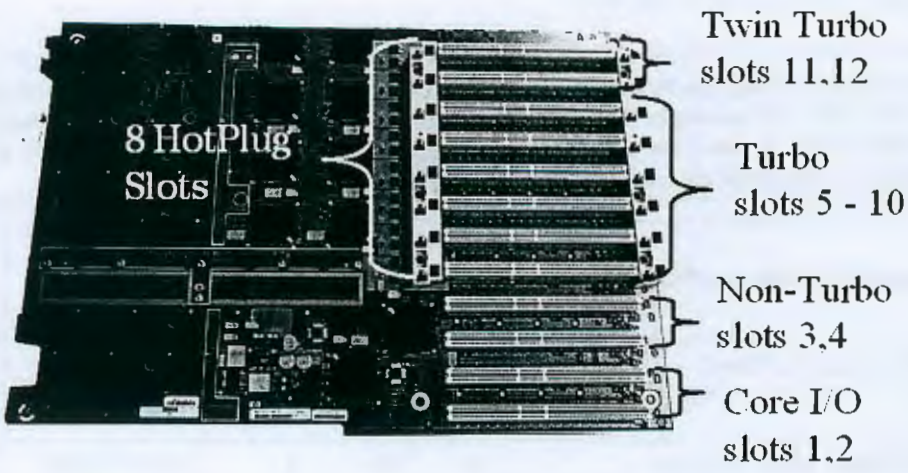
NOTE Slot 3 will become enabled on rp5400 servers with server firmware versions later than 40.48.

A slot 3 enabled label (A5576-84009) is available for rp5400 systems.

F C T
4799
Paula
A C

rp5470 PCI Card Slots

For rp5470 models, the 10 PCI I/O slots consist of Twin Turbo, Turbo, and non-Turbo slots. The following illustration shows the PCI card slot layout.



- Slots 1 and 2 are reserved for the rp54xx LAN/SCSI and GSP (Guardian Service Processor) Core I/O cards, respectively. Slots 1 and 2 are non-Turbo slots. Non-Turbo slots share a single 250MB/s PCI bus and are incapable of HotPlug functionality. The server must be turned off prior to removing or installing the LAN/SCSI or GSP cards in these slots.
- Slots 3 and 4 are non-Turbo slots. These two Non-Turbo slots share a single 250MB/s PCI bus, run at 33MHz and support 32 and 64-bit PCI cards. Non-Turbo slots are incapable of HotPlug functionality. The server must be turned off prior to removing or installing PCI cards in these slots.
- Slots 5 - 10 are Turbo slots. Each Turbo slot has a dedicated 250MB/s PCI bus, run at 66MHz and support 32 and 64-bit PCI cards. Turbo slots are HotPlug capable. Below each Turbo slot is a plastic PCI card separator. The PCI card separator has two LEDs and a pull tab on the outer edge. The LED's provide power and status for the slot. The pull tab allows the PCI card to be easily removed.
- Slots 11 and 12 are Twin Turbo slots. Each Twin Turbo slot has a dedicated 500MB/S PCI bus, runs at 66 MHz, and supports 32- and 64-bit PCI cards. Twin Turbo slots are HotPlug capable. Below each Twin Turbo slot is a plastic PCI card separator. The PCI card separator has two LEDs and a pull tab on the outer edge. The LED's provide power and status for the slot and the pull tab allows the PCI card to be easily removed.

rp5470 servers have access to all (1-12) slots.

ROS Nº 03/2005 - CN
CPMI - CORREIOS
1571
Fls:
Doc: 3701

PCI I/O Card Installation Restrictions

Restrictions apply regarding the installation of PCI I/O cards which contain a PCI-to-PCI bridge:

- HP-UX boot is currently not supported for cards that contain a PCI-to-PCI bridge.
- HP-UX patches are required when more than one card containing a PCI-to-PCI bridge is installed in non-Turbo slots.

PCI I/O Card Installation Order

The following table shows a standard factory PCI card installation that begins with slot 12. Use this table as a guideline for installing PCI I/O cards in the field.

NOTE A system shipped from the factory may have a different configuration than the same system built in the field. For example: The factory will install the graphics card in slot 12 and add other cards below. In the field, slot 12 may already be occupied by another PCI card. It is acceptable for the graphics card to be installed in any available Turbo slot.

Product Number	Description (all are PCI cards)	Max	Boot	Load Order *	Part Number	Notes
A6150A	Graphics, Graphics Card	1	No	1	A4982-66501	3,8
A5838A	Combo		No	3	A5838-60001	9
A5483A	ATM 622Mbps MMF Adapter	10	No	4	A5483-60001	10
A4926A	1000Base SX PCI LAN Adapter	10	No	5	A4926-60001	
A4926A	1000Base TX PCI LAN Adapter	10	No	6	A4926-60001	
A6092A	HYPERFabric		No	7	A6092-60001	11
A5158A	FC Tachlite		Y	8	A5846-60001	
A5486A	Praesidium Speed Card	10	No	9	A5486-60001	
A5506A	4 Port 100Base TX LAN Adapter	7/10	No	10	A5506-60101	1,2,6
A5506B	4 Port 100Base TX LAN Adapter	7/10	No	10	A5506-60102	
A5150A	Dual Port Ultra 2 SCSI adapter	10	Yes	11	A5150-60001	4
A5149A	Single Port Ultra 2 SCSI HBA	10	Yes	12	A5149-60001	
J3526A	High Perf 4 Ports Synchronous Adapter	10	No	13	5063-1322	7,5
A4800A	FWD SCSI-2 adapter	10	Yes	14	A4800-67002	
A5230A	100Base-T LAN Adapter	10	No	15	B5509-66001	
A3738A	10/100Base-T LAN Adapter	10	No	16	A3738-60001	
A3739A	Dual FDDI LAN Adapter	10	No	17	A3739-60001	
A5783A	Token Ring 4/16/100 Hardware Adapter	10	No	18	A5783-60101	

Product Number	Description (all are PCI cards)	Max	Boot	Load Order *	Part Number	Notes
J3525A	Dual Port Synchronous Adapter	10	No	19	J3525-60001	
J3593A	64 port Serial MUX system card	10	No	20	J3593-60001	
J3592A	8 Port PCI Serial MUX card	4	No	21	J3592-60101	
A6150A	Graphics, USB Card	1	No	22	A6150-60001	
A6150BX	Pinnacle 2 Graphics	1	No	1	A6150-60003	12,13
A6386A	Hyper Fabric 2 Interconnect	10	No	6	A3686-60001	
A5506A	Quad Port 10/100B-TX LAN	10	No	10	A5506-60102	14
A6749A	3.3v 64 Port Terminal MUX	10	No	24	A6749-60001	
A6748A	3.3v 8 Port Terminal MUX	10	No	25	A6748-60001	

*In top down order.

Notes:

1. Card contains a PCI-to-PCI bridge.
2. Requires PHKL_20123, PHKL_20629 and PHNE_19826 or their superseded equivalents.
3. Not supported in non-Turbo slots. Install in Turbo slots only.
4. Requires server firmware revision 39.46 or later.
5. Requires HP-UX 11.1
6. Maximum is 7 for HP-UX versions prior to 11.0. Maximum is 10 for HP-UX version 11.1 and later.
7. Requires PHKL_19543 and PHKL_19544 or their superseded equivalents.
8. Requires HP-UX 11.0 Support Plus (IPR) 0006, June 2000 or later. This product to be released 6/00.
9. Not supported in a shared slot (slots 3-4 for rp5470, slots 3-6 for rp5450, not applicable for rp5400).
10. If you are installing ATM 622 cards in an rp5470 configuration, do not install them in slots 3 and 4 (shared slots).
11. Requires 768 MB for first card and 512 MB for each additional card.
12. Not supported in shared slots.
13. Max of 1. Needs USB card for keyboard and mouse.
14. Contains PCI bridge.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1572
Fls:
Doc:
3701

Installing a PCI Card

Follow these procedures to install a PCI card.

Step 1. Power down and unplug the rp54xx server.

NOTE DC voltages are present when the server is connected to AC power. Do not attempt to install or service: CPUs, Memory, PSMs, the Platform Monitor or PCI I/O cards installed in non-Turbo slots (1-6) while DC voltage is present. Failure to observe this warning may result in damage to the server.

Step 2. Make the right side of the server accessible for service.

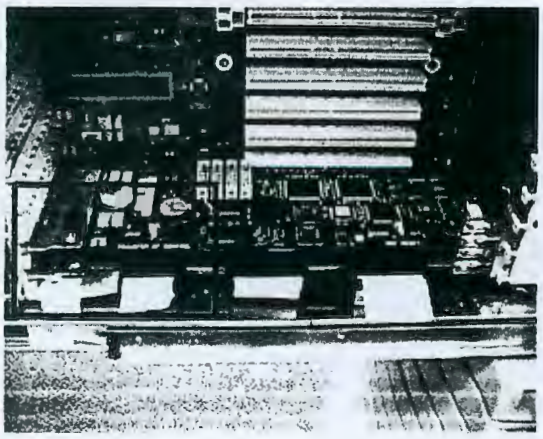
Step 3. Using a Torx 15 screwdriver, loosen the captive screws on the right side panel. This panel has a label which shows which PCI I/O slots are available and the corresponding paths. The PCI I/O slot paths for rp5400, rp5450, and rp5470 are shown below.

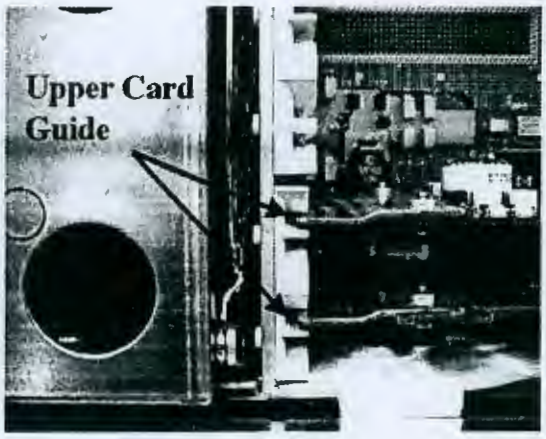
Slot	rp5400		rp5450		rp5430/rp5470	
	Slot Type	**Path**	**Slot/Type**	**Path**	**Slot Type**	**Path**
12	**Turbo**	**0/4/0**	**Turbo**	**0/4/0**	**Twin Turbo**	**0/10/0**
11	Turbo	0/7/0	Turbo	0/7/0	Twin Turbo	0/12/0
10	Turbo	0/3/0	Turbo	0/3/0	Turbo	0/8/0
9	Turbo	0/6/0	Turbo	0/6/0	Turbo	0/9/0
8	Turbo	0/2/0	Turbo	0/2/0	Turbo	0/3/0
7	Not Available		Turbo	0/5/0	Turbo[a]	0/1/0
6	Not Available		Shared	0/1/0	Turbo[a]	0/5/0
5	Not Available		Shared	0/1/1	Turbo[a]	0/2/0
4	Not Available		Shared	0/1/2	Shared[a]	0/4/0
3	Not Available[b]		Shared	0/1/3	Shared	0/4/2
2	GSP		GSP		GSP	
1	LAN/SCSI		LAN/SCSI		LAN/SCSI	

a. Slot is NOT AVAILABLE for rp5430.
b. Slot 3 becomes available with server firmware versions later than 40.48.

Step 4. Remove the PCI slot cover from the slot that will receive the PCI card. To remove the PCI slot cover, slide the PCI slot cover away from the server.

Step 5. Slide the PCI card connectors into the slot, snapping firmly in place. For full length (cards that extend to the left side card guides) PCI cards, use the UPPER card guide.





Step 6. At the rear of the chassis, connect the I/O cable to the card just installed.

Step 7. Replace the right side panel and tighten the captive screws.

Step 8. For rack configurations, insert the rp54xx server back into the rack.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1573
Fls:
3701
Doc:

Step 9. For deskside enclosure configurations, replace the deskside enclosure cover.

Step 10. Power the server on.

Step 11. Use the server firmware `in io` command to verify the PCI cards are recognized by the server. If AUTOBOOT is ON, it will be necessary to interrupt the boot process to get to the server firmware `Main Menu: Enter command or menu >` prompt.

Step 12. Boot HP-UX and run the `ioscan` utility to verify the system recognizes the new PCI card.

Online Addition/Replacement (OLA/R) of PCI I/O cards

Beginning with HP-UX 11i (11.11) rp54xx servers support the on-line addition and replacement of PCI I/O cards. In order for this high availability feature to be fully implemented, the following server requirements must be met:

- rp5400A/rp5450A firmware must be later than 40.26 (rp5400B/rp5450B/rp5470A firmware will support OLA/R upon its release).
- HP-UX operating system must be 11i (11.11) or later.

There is a bit that the HP-UX operating system examines to determine if the server hardware and firmware is capable of OLA/R. This bit is controlled by server firmware. If the bit is ON, OLA/R is possible (when requirements have been met). The bit was mistakenly set to ON for all rp5400 and rp5450 revision A (rp5400A and rp5450A) servers. As a result, HP-UX may incorrectly identify these models as being OLA/R capable. In order to avoid this confusion, verify that the correct level of server firmware is installed.

E C T
4493
Paulo
A C

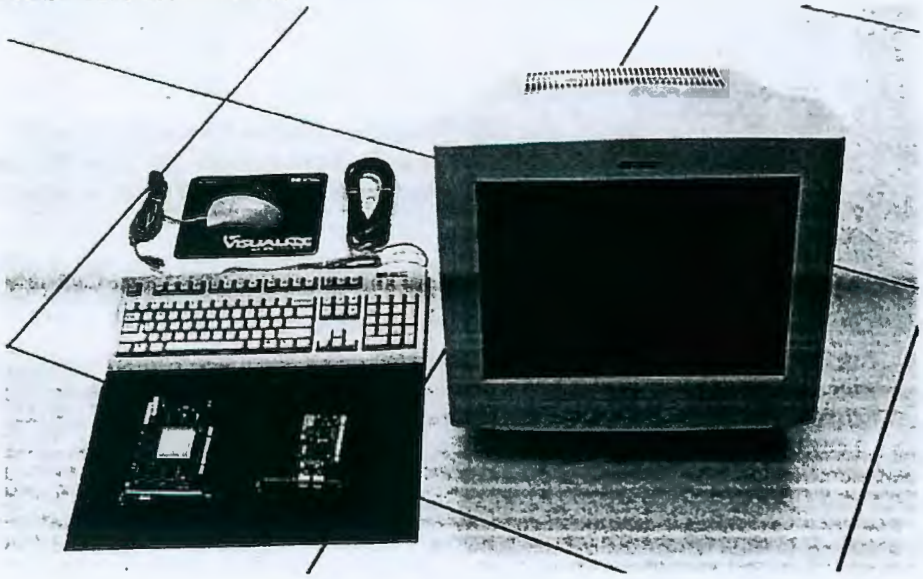
Installing Graphics

This section explains how to install rp54xx 2D graphics hardware. For a complete graphics solution, three products are required. The products listed below are the only products supported on rp54xx servers.

- A6150A rp54xx Graphics Package
  - — Includes PCI graphics card
  - — Includes PCI USB (Universal Serial Bus) card
- A4983B Keyboard and Mouse Kit
  - — Includes mouse with 114" cable
  - — Includes keyboard with 109" cable
- D8910W (19") or D2847W (21)" Monitor
  - — Includes localized power cord and 75" 15-pin video cable

NOTE rp54xx graphics requires HP-UX 11.0 Support Plus (IPR) 0006, June 2000 or later.

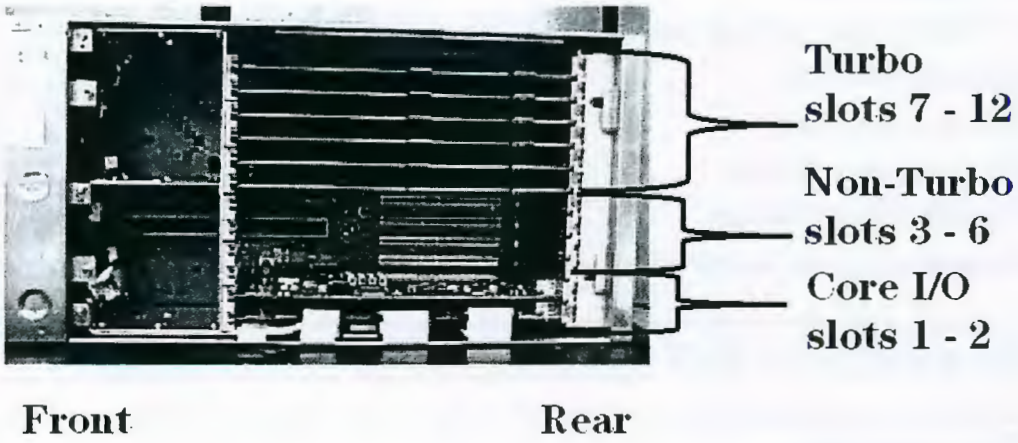
The photo below includes the A6150A, A4983B and D8910W products. The video cable for the monitor is not shown. Black ESD mat not included.



RQS Nº 03/2005 - CN
CPMI - CORREIOS
1574
Fls:
3701
Doc:

rp54xx servers have a total of 12 PCI I/O slots. Slots 1 and 2 are reserved for the LAN/SCSI and GSP Core I/O cards, leaving 10 PCI I/O slots available for Customer use. These 10 PCI I/O slots consist of Turbo and non-Turbo slots.

rp54xx PCI Slots



- Slots 1 and 2 are reserved for the rp54xx LAN/SCSI and GSP (Guardian Service Processor) Core I/O cards, respectively. Slots 1 and 2 are non-Turbo slots. Non-Turbo slots share a single 250MB/s PCI bus. Non-Turbo slots are incapable of HotPlug functionality. The server must be turned off prior to removing or installing the LAN/SCSI or GSP cards in these slots.
- Slots 3 - 6 are non-Turbo slots. These four Non-Turbo slots share a single 250MB/s PCI bus, run at 33MHz and support 32 and 64-bit PCI cards. Non-Turbo slots are incapable of HotPlug functionality. The server must be turned off prior to removing or installing PCI cards in these slots.
- Slots 7 - 12 are Turbo slots. Each Turbo slot has a dedicated 250MB/s PCI bus, run at 66MHz and support 32 and 64-bit PCI cards. Turbo slots are HotPlug capable. Below each Turbo slot is a plastic PCI card separator. The PCI card separator has two LEDs and a pull tab on the outer edge. The LED's provide power and status for the slot. The pull tab allows the PCI card to be easily removed.

rp5400 servers can access PCI slots 1,2 and 8-12. rp5450/3000 servers can access all PCI slots.

Follow these procedures to install graphics cards.

Step 1. Install HP-UX 11.0 Support Plus (IPR) 0006, June 2000 or later. This step ensures the appropriate HP-UX drivers are installed.

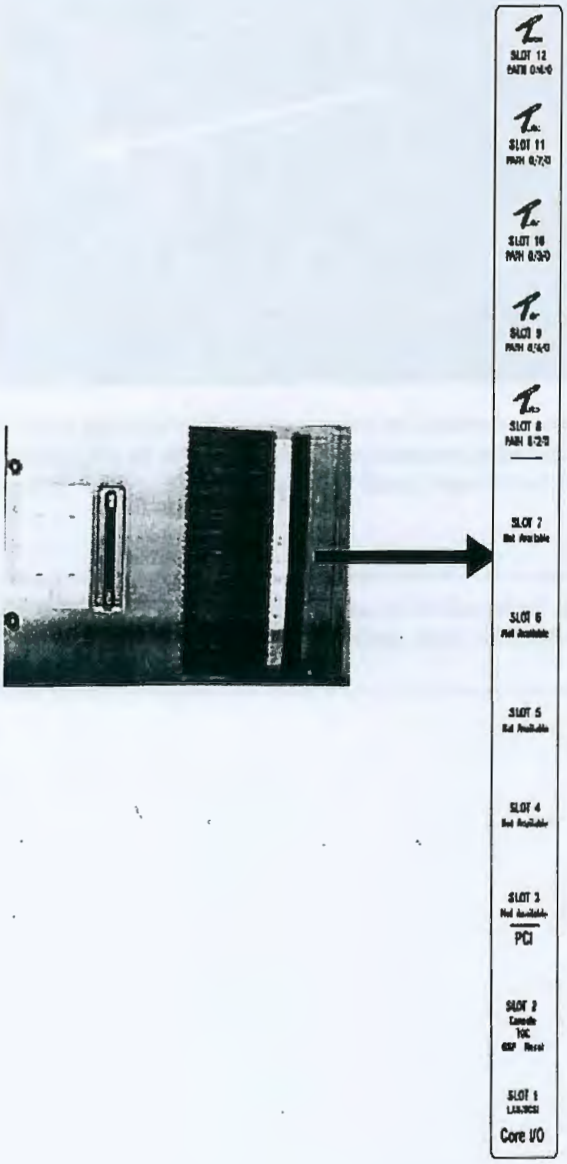
Step 2. Power down and unplug the rp54xx server.

E C T
4191
Paula
A C

NOTE DC voltages are present when the server is connected to AC power. Do not attempt to install or service: CPUs, Memory, PSMs, the Platform Monitor or PCI I/O cards installed in non-Turbo slots (1-6) while DC voltage is present. Failure to observe this warning may result in damage to the server.

Step 3. Make the right side of the server accessible for service.

Step 4. Using a Torx 15 screwdriver, loosen the captive screws on the right side panel. This panel has a label which shows which PCI I/O slots are available and the corresponding paths. The label shown below is for an rp5400.



RQS Nº 03/2005 - CN
CPMI - CORREIOS
1535
Fls: A
Doc: 3701

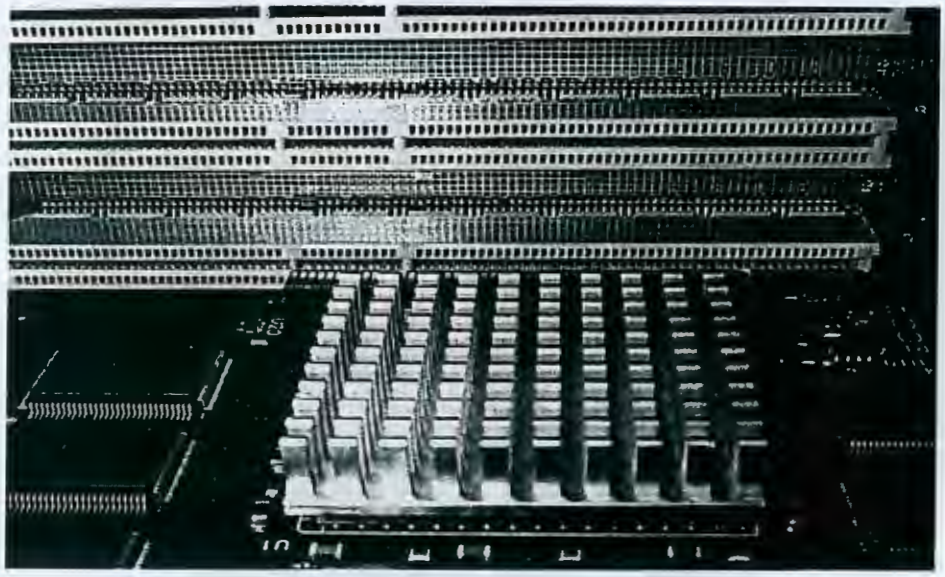
Step 5. Grasp the handle on the right rear panel and remove the panel from the side of the chassis. The 12 PCI slots, numbered 1-12 from bottom to top, will be in view.

Step 6. Remove the PCI slot cover from the slot that will receive the PCI card. To remove the PCI slot cover, slide the PCI slot cover away from the server.

Step 7. Center the graphics card within the space created by removing the PCI I/O slot cover. Slide the card toward the edge connectors. Ensure the edge connectors on the card are in alignment with the connectors of the slot. Apply pressure to the card until it snaps firmly in place. Repeat process for USB card.

NOTE The graphics card must be installed in any Turbo slot while the USB will work in any slot. To reserve Turbo slots for high performance I/O cards, install the USB card in a non-Turbo slot

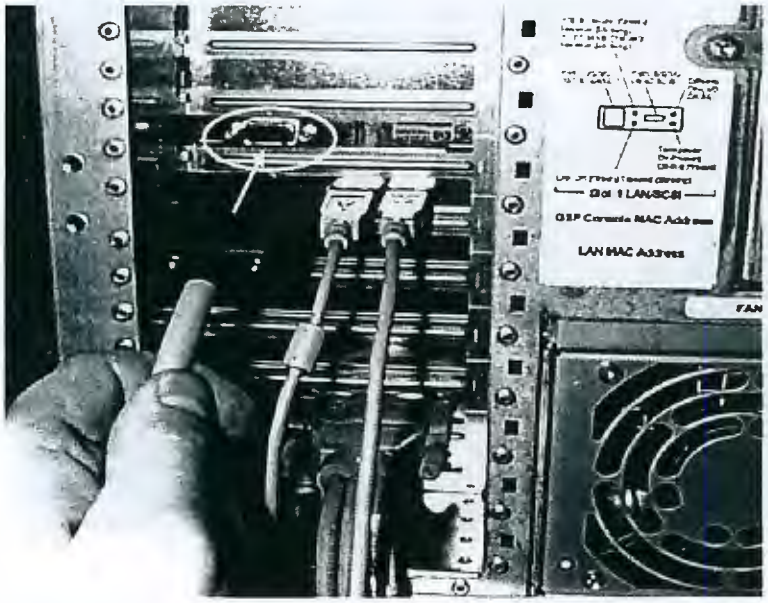
---



Step 8. At the rear of the chassis, connect the keyboard and mouse cables to the USB card. It does not matter which connector is used for the keyboard or mouse.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1576
Fls:
3701
Doc:

Step 9. Connect one end of the 15-pin video cable connector on the graphics card. This connector is labeled "Graphics Display" and "Video Out". Connect the other end of this cable to the graphics monitor.



Step 10. Replace the right side panel and tighten the captive screws.

Step 11. For rack configurations, insert the rp54xx server back into the rack.

Step 12. For deskside enclosure configurations, repalce the deskside enclosure cover.

Step 13. Power the server on.

Step 14. Use the server firmware `in io` command to verify the graphics cards are recognized by the server. If AUTOBOOT is ON, it will be necessary to interrupt the boot process to get to the server firmware `Main Menu: Enter command or menu >` prompt.

Step 15. Boot HP-UX and run the `ioscan` utility to verify the system recognizes the new PCI card.

Step 16. Logon as root and install X/CDE/Motif if not already installed.

Graphics Troubleshooting

This section describes how to troubleshoot common problems encountered during installation or attempted use of graphics. The following system utilities can be used to display or set the graphics configuration:

- `/opt/graphics/common/bin/graphinfo` allows you to display the current graphics configuration and the graphics drivers that are being used.
- `/opt/graphics/common/bin/setmon` allows you to reconfigure the monitor type.
- The `display` menu of the HP-UX System Administration Manager (SAM) utility allows you to configure the X-Server and set the monitor type.

  On-line diagnostics provide information, verify and diagnose coverage for the graphics and USB cards.Off-line diagnostics do not exist for either the graphics or USB card.
- The HP-UX `ioscan` utility can be used to verify the HP-UX operating system recognized the hardware.

Symptom: CDE will not come up.

Step 1. Ensure /dev/crt was created. If not created, use `insf -e` to create.

Step 2. Ensure the system is at run level 3. Use `who -r` to determine run level. Use `init 3` to change to run level 3.

Step 3. Ensure dt is enabled. Use `/usr/dt/bin/dtconfig -e` to enable dt.

Step 4. Ensure /etc/dt/config/Xservers exists. If not, use `/usr/dt/config/dtrc.d/20_graph_conf` to create.

Step 5. Ensure the line: * Local local@console /usr/bin/X11/X :0 is not commented out of the /etc/dt/config/Xservers file.

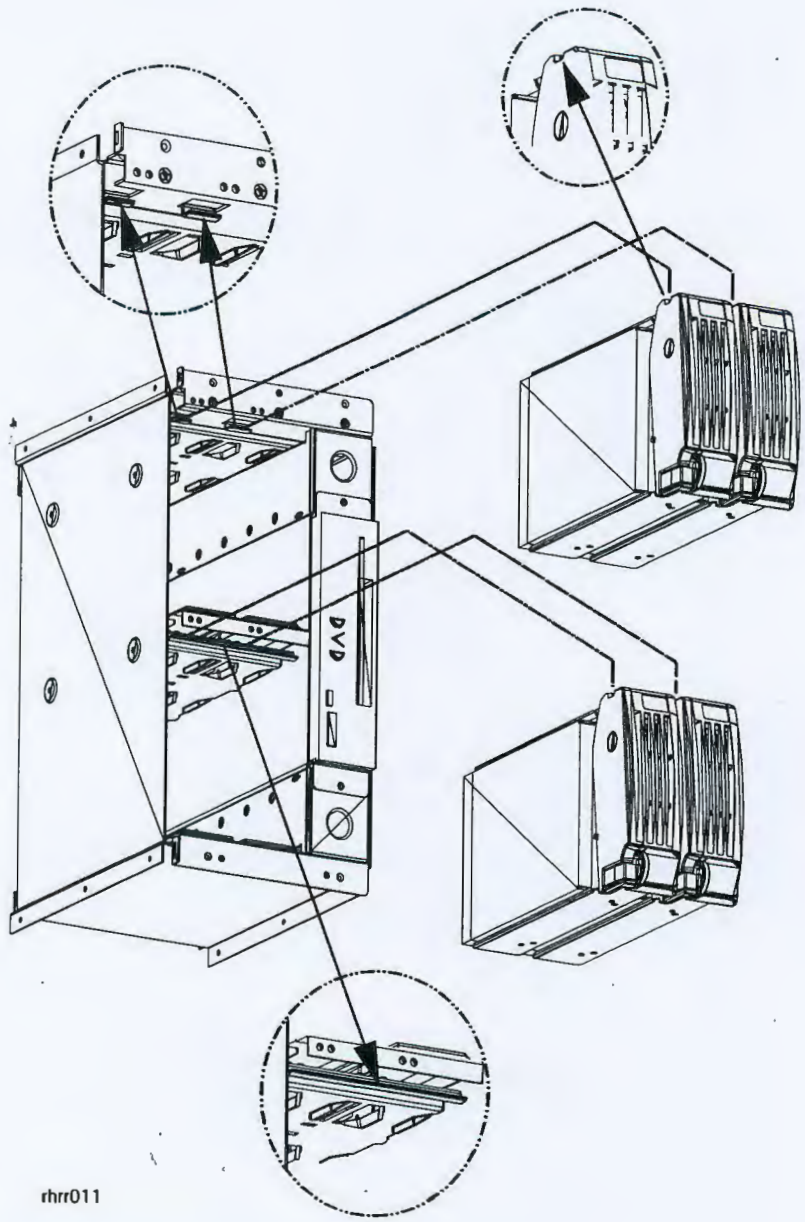
Step 6. Reboot HP-UX.

Symptom: HP-UX does not recognize the graphics cards. `unknown` appears in the ioscan output for these cards

Step 1. Examine the output of the `swlist` command to ensure the correct version of HP-UX is installed.

Step 2. Update HP-UX as necessary

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1577
Fls:
3701
Doc:



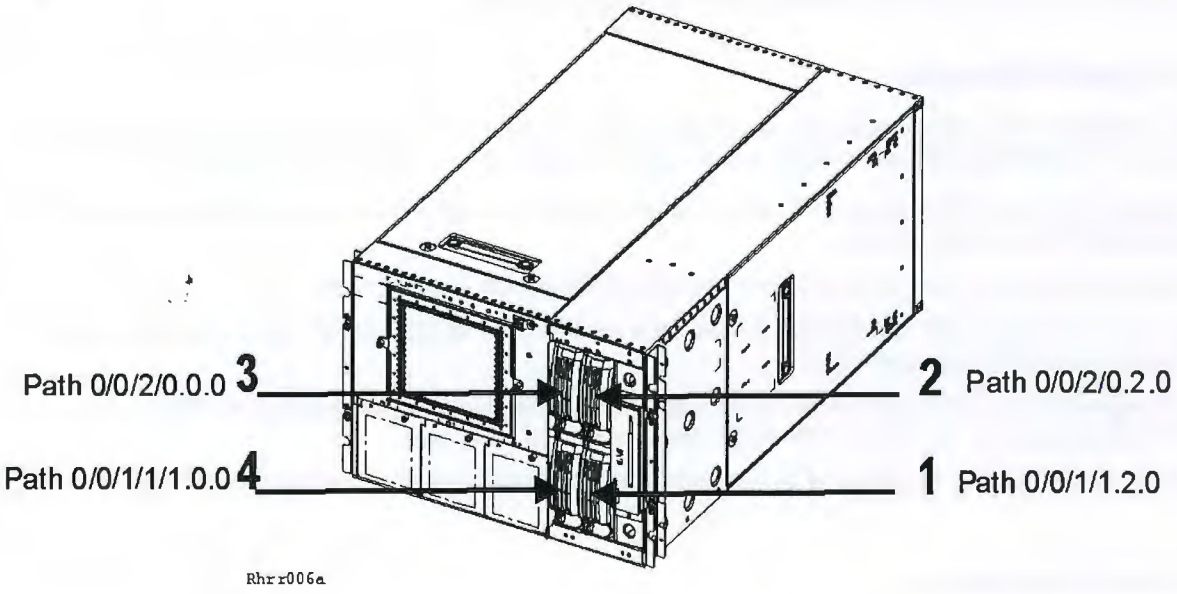
Step 4. Secure the connection by pushing the blue release lever closed.

Step 5. Refer to HP-UX documentation to configure the new disk.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1578
Fls:
Doc: 3701

Installing Disk Drives

rp54xx servers support up to four optional internal hard drives. These drives must be installed in the following sequence:



It is not necessary to shutdown the HP-UX operating system or power off the server to install a new disk. Follow this procedure to add internal hard disk drives to your rp54xx server.

Step 1. If a front bezel is installed on the face of the server, open the right-hand panel to gain access to the disk slots.

Step 2. Remove the disk drive slot cover.

Step 3. Insert the new disk drive into the slot until the rear connectors snap into place in the card guide. As shown in the following graphic, the notches at the top of the disk drives must snap over the small brackets in the disk bay to ensure a firm connection.

E C T
C P L 1783 Paula A C

4 Cable Connections

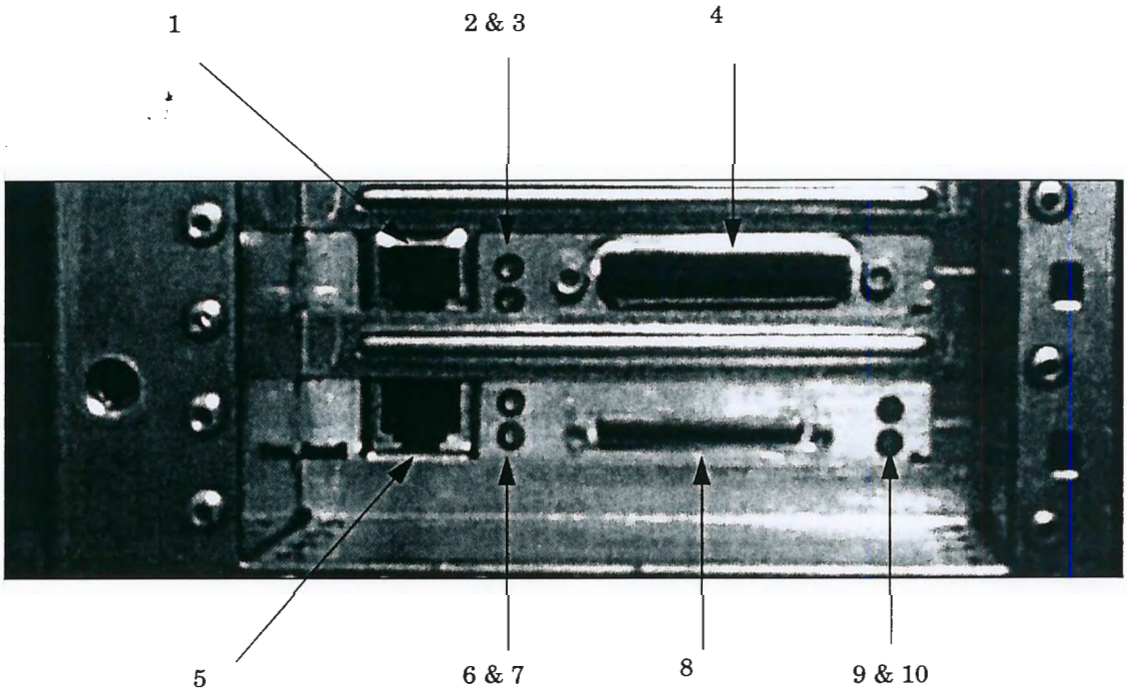
RQS Nº 03/2005 - CN
CPMI - CORREIOS
1579
Fls:
Doc: 3701

Core I/O Connections

The following paragraphs describe the indicators and connections of the rp54xx Core I/O. Core I/O consists of a LAN/SCSI card in slot 1 (lower slot in graphic) and a Guardian Service Processor (GSP) in slot 2 (upper slot in graphic). There are two versions of GSP, revision A and revision B.

Revision A GSP

The following graphic shows the indicators and connectors for the revision A GSP and LAN/SCSI Core I/O boards.



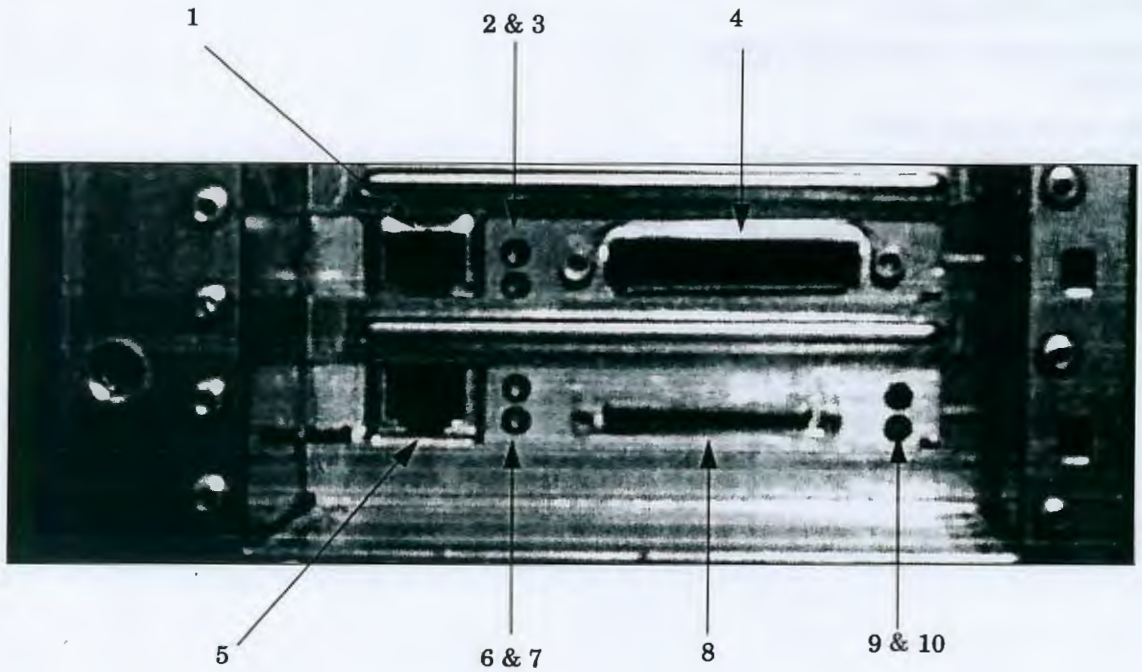
1. 10-Base-T LAN (RJ-45) Connector
   GSP LAN.
2. Green/Red (Upper LED)
   Green = GSP Power On.
   Flashing Green = LAN Receive.
   Red = Guardian Support Processor Test Failed.
3. Green/Red, (Lower LED)
   Green = Link OK.
   Flashing Green = LAN Transmit.
   Red = Guardian Support Processor Test Failed.
4. Console/UPS/Remote Connector (D-Type 25-Pin female).
   Requires an A5191-63001 "W" adapter cable
5. 10/100 Base-T = Primary LAN (RJ-45) Connection
   Path 0/0/0/0

4.781

6. Green/Yellow (Upper LED)
   Green = 100 Base-T Mode
   Green Blinking = 100 Base-T Receiving
   Amber = 10 Base-T Mode
   Amber Blinking = 10 Base-T Receiving
7. Green (Lower LED)
   Green = Link OK (10/100 Base-T Mode indicated by LED #6)
   Green Blinking = Transmitting
8. Ultra-2 SCSI Connector (68-Pin VHDCI SCSI)
   Path 0/0/1/0
9. SCSI Mode (Green, Upper LED)
   On = Low Voltage Differential (LVD) Mode.
   Off = Single Ended Mode.
10. SCSI Terminator Power (Amber, Lower LED)
    On = Terminator power present
    Off = Terminator power Not present.

Revision B GSP

The following graphic shows the indicators and connectors for the revision B GSP and LAN/SCSI Core I/O boards.



ROS Nº 03/2005 - CN
CPMI - CORREIOS
1580
Fls:
3701
Doc:

1. 10/100-Base-T LAN (RJ-45) Connector.
   GSP LAN.
2. Green/Red (Upper LED).
   Green = GSP Power On.
   Red = Guardian Support Processor Test Failed.
3. Green/Yellow, (Lower LED).
   Green = 100 Base-T Link OK.
   Flashing Green = 100 Base-T LAN Activity.
   Yellow = 10 Base-T Link OK.
   Flashing Yellow = 10 Base -T LAN Activity.
4. Console/UPS/Remote Connector (D-Type 25-Pin female).
   Requires an A6144-63001 "M" adapter cable.
5. 10/100 Base-T = Primary LAN (RJ-45) Connection.
   Path 0/0/0/0.
6. Green/Yellow (Upper LED).
   Green = 100 Base-T Mode.
   Green Blinking = 100 Base-T Receiving.
   Amber = 10 Base-T Mode.
   Amber Blinking = 10 Base-T Receiving.
7. Green (Lower LED).
   Green = Link OK (10/100 Base-T Mode indicated by LED #6).
   Green Blinking = Transmitting.
8. Ultra-2 SCSI Connector (68-Pin VHDCI SCSI).
   Path 0/0/1/0.
9. SCSI Mode (Green, Upper LED)
   On = Low Voltage Differential (LVD) Mode.
   Off = Single Ended Mode.
10. SCSI Terminator Power (Amber, Lower LED)
    On = Terminator power present
    Off = Terminator power Not present.

Guardian Service Processor (GSP) Overview

This section provides an overview of the Guardian Service Processor (GSP). The GSP is an always on, dedicated service processor that monitors system power, cooling and configuration, and provides console communications. Power and cooling information is obtained via an interface to the platform monitor card. Configuration information is obtained via connection to the Serial Presence Detect (SPD) bus. The GSP can only be installed in slot 2 and must be present for the server to power up.

The GSP has downloadable firmware which can be updated independent of the HP-UX operating system. GSP firmware updates can occur anytime the GSP is active. If the DC power switch is OFF, the GSP is still operational and GSP firmware updates can still occur. GSP firmware updates may be performed by customers.

If the GSP becomes hung, it is possible to reset the GSP without impacting the server. The GSP may be reset via the GSP RESET button on the right side of the card. The PCI cover panel (right side panel) must first be removed to allow access to the right side if the GSP card.

The GSP has two connectors on the bulkhead. An RJ-45 for LAN connections and a female DB25 connector for RS-232 connections. Attach either a "W" or an "M" cable to the DB25 connector to provide individual output for CONSOLE, REMOTE and UPS.

To access the GSP from the local ASCII console, type control b and the `GSP>` prompt will appear. It may be necessary to type control Ecf first. To exit the GSP, type `GSP>co`.

The GSP was originally a core component of the revision A rp5400 (A5576A) and rp5450 (A5191A) servers. Beginning with introduction of the revision B rp5400 (A5576B), rp5450 (A5191B), and rp5470 servers the GSP became a separate, must order product (A6696A).

There are two revisions of rp54xx GSP: rev A (A6696A) and rev B (A6696B). Both GSPs must be installed in order for the server to power up.

GSP LAN

This LAN is exclusively for LAN console access and is not configurable via HP-UX. The LAN is configured via GSP commands. Hostname, IP, gateway and subnet mask parameters may be set via the `GSP>lc` command. The GSP may also initiate ping via the `GSP>xd` command.

GSP RS-232

The DB25 connector on the GSP is used for RS-232 communications to a local console (via CONSOLE connector), a remote console via modem (REMOTE connector), and a UPS (UPS connector). The baud rate, term type, etc., of the CONSOLE and REMOTE ports are configured via `GSP>ca` command.

The GSP supports VT100 and HPTERM terminal emulation. For correct communications, the GSP and RS-232 device must use the same terminal emulation and baud rates.

GSP Features

The revision A GSP provides a 10 base-T LAN connector for LAN console access and a DB-25 connector to which the A5191-63001 W-cable connects. The W-cable provides REMOTE, UPS, and CONSOLE DB-9 connectors.

Features of the revision A GSP are:

- 10 Base-T LAN connector for revision A GSP

ECT 4.770 CPL AC
ECT CPL AC
ROS Nº 03/2005 CN
CPMI - CORREIOS
1581
Fls:
Doc: 3701

- 10/100 Base-T LAN connector for revision B GSP
- On-board processor dedicated to GSP functions
- Error logging and notification
- Display of system alerts and selftest chassis codes
- Powered by 15 VDC housekeeping power that is present when the front panel switch is off
- Power and configuration monitoring
- RS-232, LAN, REMOTE and WEB console access
- Administrator and user security
- Alphanumeric paging.

There are two revisions of rp54xx GSP: revision A (A6696A) and revision B (A6696B). Due to significant hardware differences between the revision A and B GSP, each GSP requires it's own firmware. Revision A GSP firmware can only be installed in a revision A GSP and revision B GSP firmware can only be installed in a revision B GSP. The hardware differences are necessary to incorporate the embedded web access, 10/100 Base-t LAN, and faster GSP processor.

The GSP provides four types of console access: RS-232, Remote, LAN and Web. Console information is mirrored to all four console types. Refer to *Configure System Console* for more information.

The GSP was originally a core component of the revision A rp5400 (A5576A) and rp5450 (A5191A) servers. Beginning with introduction of the revision B rp5400 (A5576B), rp5450 (A5191B), and rp5470 servers the GSP became a separate, must order product (A6696A).

Revision A GSP

The revision A GSP is identified by product number A6696A and part numbers: A5191-60012, A5191-69012, and A5191-69112.

The revision A GSP requires a "W" cable to be attached to the DB25 connector. The part number of the "W" is A5191-63001. The "W" cable provides female DB9 connectors for CONSOLE, REMOTE and UPS. The maximum supported baud rate for the CONSOLE and REMOTE connectors is 19200 baud and 1200 baud for the UPS.

The paths for the CONSOLE, UPS, and REMOTE are 0/0/4/0.0, 0/0/4/0.1, and 0/0/4/0.2 respectively.

For the rev A GSP, the web console is accomplished by shipping one J3591A Secure Web Console with each rp54xx server. The Secure Web Console can be used in place of an ASCII console to provide console access via a web connection. If you are installing an rp54xx server that does not have an ASCII console, you may use the Secure Web Console as the console. However, you must first configure the Secure Web Console. Refer to *Secure Web Console Installation and Configuration* for more information on SWC Installation/Configuration.

Revision B GSP

The revision B GSP is identified by product number A6696B and part numbers: A6144-60012, A6144-69012, and A6144-69112.

The revision B GSP requires an "M" cable to be attached to the DB25 connector. The part number of the "M" cable is A6144-63001. The "M" cable provides female DB9 connectors for CONSOLE, REMOTE, and UPS. The maximum supported baud rate for the CONSOLE and REMOTE connectors is 38400 baud and 1200 baud for the UPS.

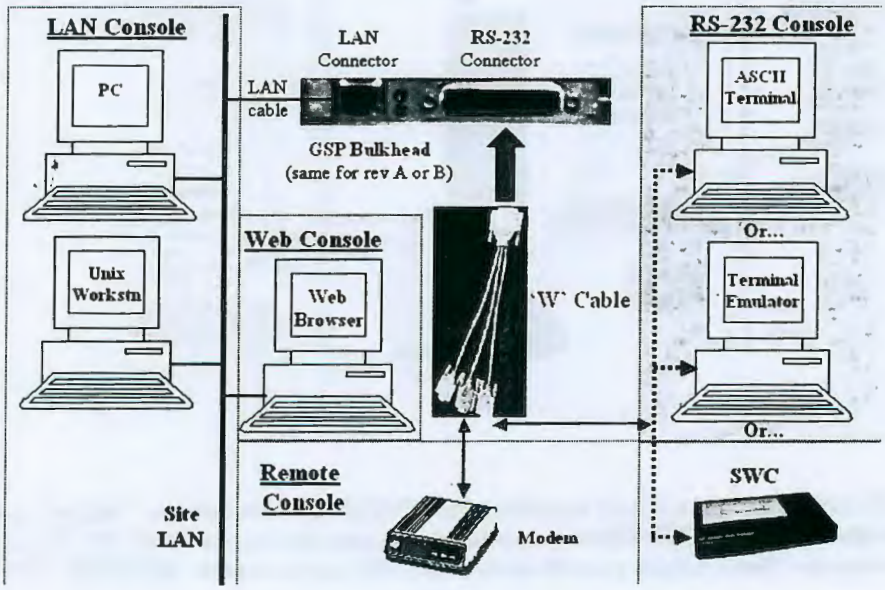
The paths for the CONSOLE, UPS, and REMOTE are 0/0/4/1.0, 0/0/4/1.1 and 0/0/4/1.2 respectively.

ECT
4.777
J
AC

Configure System Consoles

rp54xx servers provide RS-232, REMOTE, LAN and WEB console access. All console access involves the Guardian Service Processor (GSP). rp54xx servers use either a revision A or revision B GSP. Below is an illustration of the console access provided by the revision A GSP.

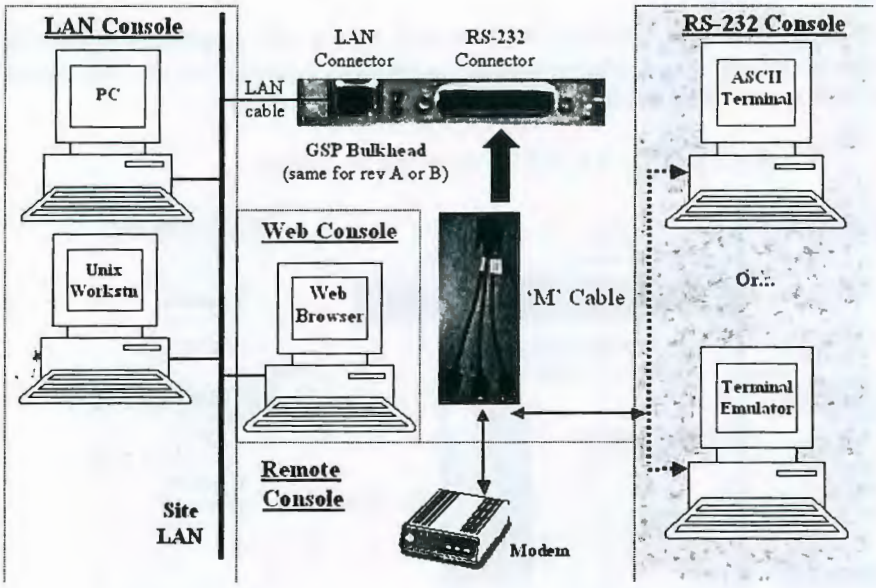
Revision A GSP Console Access



The revision B GSP has embedded web access, eliminating the need for an external Secure Web Console (SWC). Below is an illustration of the console access provided by the revision A GSP.

ROS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1582
Doc: 3701

Revision B GSP Console Access



GSP Cables

Both the revision A and B GSPs provide a DB-25 connector for RS-232 communications. Connect the A5191-63001 W- cable to the revision A GSP DB25 connector or connect the A6144-63001 M-cable to the revision B GSP DB25 connector. These cables provide individual DB9 connectors for REMOTE, UPS and CONSOLE.

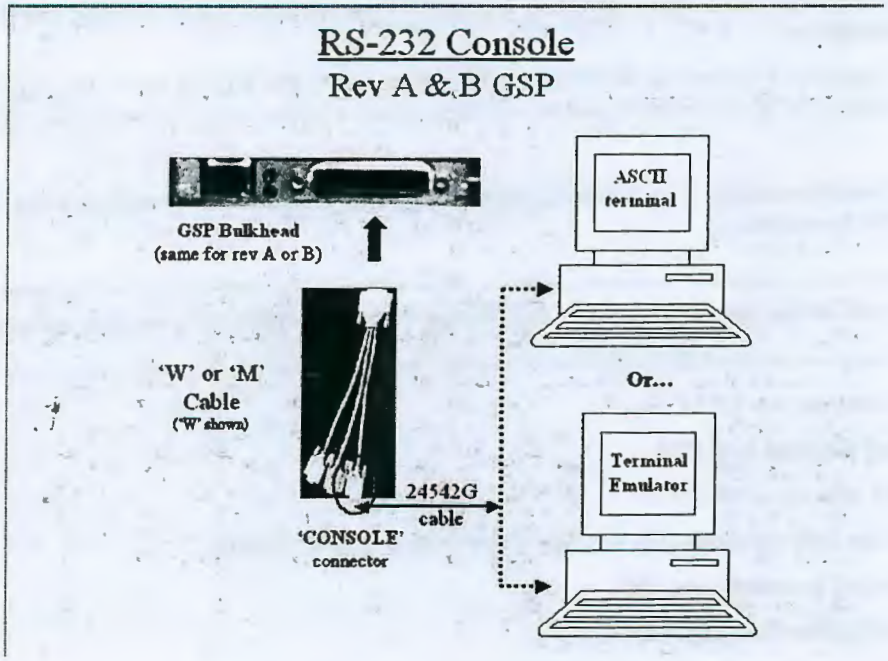
NOTE Use the A5191-63001 W-cable with revision A GSP and A6144-63001 M-cable with revision B GSP *only*. Failure to use the right cable can result in reduced functionality.

The W and M-cables are slightly different. The W-cable has full RS-232 capability on the REMOTE and CONSOLE connectors and partial RS-232 capability on the UPS connector. The M-cable has full RS-232 capability on the REMOTE and UPS connectors and partial RS-232 capability on the CONSOLE connector. The cable change is to be consistent with rp54xx functionality. The cables are different colors to easily tell them apart. The W-cable is gray and has part number A5191-63001. The M-cable is black and has part number A6144-63001.

Configure RS-232 Console

The physical connections for an RS-232 console include attaching the correct cable to the GSP. Next, connect the 24542G cable (supplied) to the CONSOLE connector and the serial port of the ASCII console. A personal computer (PC) running terminal emulation software may be used in place of an ASCII console. Refer to the illustration below for RS-232 console.

ECT
4.775
J.
AC



Step 1. The GSP is located in slot 2 of the rp54xx' rear card cage. Connect the 25-pin end of:

- the A5191-63001 W-cable to the 25-pin connector on the revision A GSP card (A5191-60012) OR
- the A6144-63001 M-cable to the 25-pin connector on the revision B GSP card (A6144-60012)

Step 2. Connect the 9-pin "Console" connector of either the W or M-cable to the 9-pin D-type connector of a 24542G RS-232 cable.

Step 3. Connect the 25-pin end of the 24542G serial cable to the serial/RS232 port on the ASCII console. (RS232 Serial Port labeling may vary depending on manufacturer.)

Step 4. Connect the System Console to input AC power.

Step 5. Turn the System Console AC power switch to ON.

After the physical connections have been made, configure the ASCII console. When using the C1099A Terminal Console, the default settings are recommended. Refer to the C1099A Terminal Console operating manual for instructions on how to obtain default settings.

The HP 700 series console may also be used as an ASCII console. Both the C1099A Terminal Console and S700 consoles support HPterm and VT100 emulations. The emulation of the GSP and ASCII console need not match for communications between them to occur. However, to ensure proper communications, HP recommends the ASCII console and GSP use the same emulation. HP also recommends that other configurable parameters on the GSP match those of the ASCII console. Baud rate, start/stop bits, etc... The default emulation of the GSP is VT100.

Below is a procedure to configure a HP 700 serial console for VT100 emulation.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
55
1583
Fls:
3701
Doc:

HP 700 Series System Console Configuration

The following describes the steps required to configure the HP 700 series terminal for VT-100 mode for operation with an rp54xx server.

Although any terminal capable of operating in VT-100 mode can be used, the HP700 series terminal is used here as an example because it is fairly common and it's configuration is typical of many terminals currently in use.

HP700 VT-100 Mode Configuration The following procedure outlines the steps to configure the HP700 series terminal for VT100 operation.

NOTE You may use either the arrow keys or the tab key to move between the setting options on the screen.

---

1. Press **[config keys]** function key. **[f8]**
2. Press **[terminal config]** function key. **[f5]**
3. Move to *Terminal ID* and enter "vt100".
4. Move to *Set TermMode* and, using the **[Prev]** and **[Next]** keys, select "EM100".
5. Press the **[config keys]** function key. **[f8]**
6. Press the **[ansi config]** function key. **[f6]**
7. Move to "multipage" and, using the **[Prev]** and **[Next]** keys, select "yes". (Enables screen scrolling).
8. Move to *Backspace Del* and, using the **[Prev]** and **[Next]** keys, select "Backspace/Del".
9. Move to *EM100 ID* and, using the **[Prev]** and **[Next]** keys, select "EM100".

Configure the Asynchronous Values of the GSP

After the ASCII console has been configured and physical connections made, make any necessary changes to the asynchronous values of the GSP.

1. Access the GSP with the ctrl+b entry. The GSP will respond with a `GSP>` prompt.
2. At the GSP prompt, enter the Configure Asynchronous (ca) command:

The ca command will start a series of prompts. Respond to each prompt with the appropriate information.

Example 4-1 CA command

```
Leaving Console Mode - you may lose write access. When Console Mode returns, type
^Ecf to get console write access.

GSP Host Name:  fesrhapgsp

GSP> ca

CA This command allows you to modify the local and remote modem serial
portconfigurations.

Current configuration settings:

Local Console Serial Port bit rate: 9600 bits/s

Local Console Serial Port Flow Control: Software
```

E C T
4.7731
CPL AC

```
Local Console Serial Port Terminal Type: vt100
Remote Console Serial Port Modem Protocol: CCITT  Remote Console Serial Port Modem
bit rate: 19200 bits/s
Remote Console Serial Port Modem Flow Control: Software
Remote Console Serial Port Modem Transmit Configuration Strings: Enabled
Remote Console Serial Port Modem Presence: always connected
Do you want to modify the Local Console Serial Port settings? (Y/[N])
Do you want to modify the Remote Console Serial Port Modem settings? (Y/[N])
GSP Host Name:  fesrhapgsp
```

If necessary, use the GSP help facility by typing `GSP>he`. Once in the help facility, type the command need help with. Use LI for a list of commands.

The following baud rates are recommended for the revision A GSP:

- Console: 19200
- Remote: 19200
- UPS: 1200

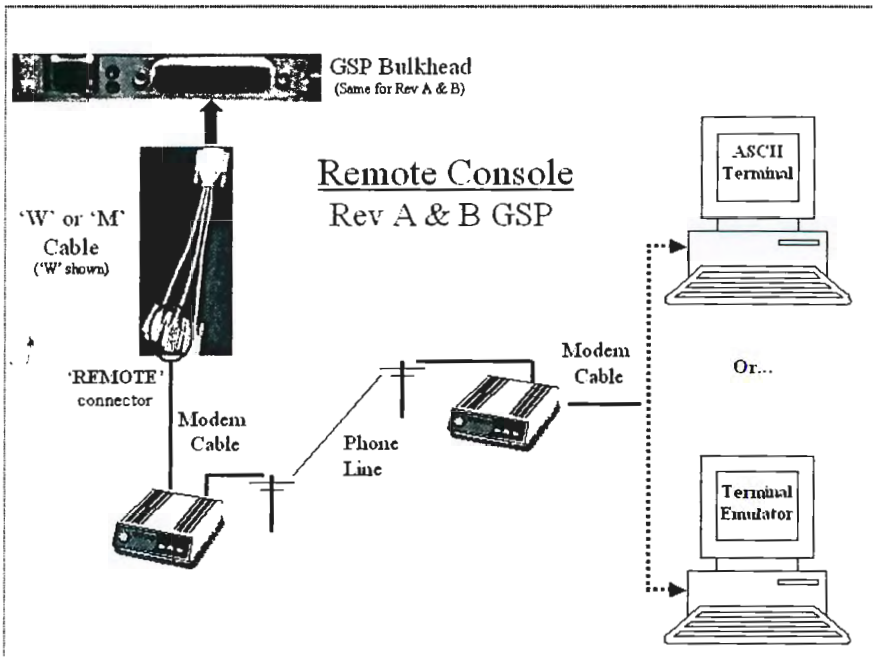
The following baud rates are recommended for the revision B GSP:

- Console: 38400
- Remote: 38400
- UPS: 1200

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1584
Fls:
3701
Doc:

Configure Remote Console

The remote console allows console access via modem connections. Below is an illustration of the REMOTE console.

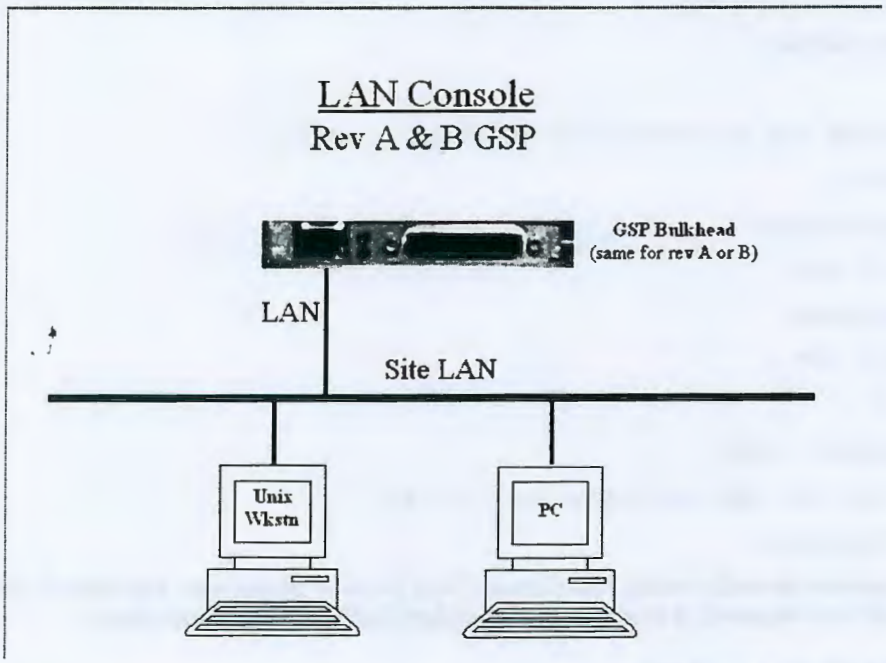


The GSP>ca command is used to configure asynchronous settings for the REMOTE console. Baud rates and emulations should match between the modems, remote ASCII terminal and the GSP. Refer to, "Configure RS232 Console" for information about setting these values.

ECT 4.767/11 CPL AC

Configure the LAN Console

The LAN console allows you to access the console from the LAN using TelNet or http (revision B GSP only) protocols. Below is an illustration of the LAN console.



The configuration of the LAN console of both the revision A and B GSPs may be done from either an ASCII console or the external Secure Web Console. For the revision B GSP, an IP may be assigned via LAN by pinging the LAN from a PC or workstation.

Configuring the GSP LAN Port via an ASCII console

The LAN port of the GSP allows connection via TelNet or http connections. Once the LAN parameters are configured, the console may be accessed via a TelNet connection or via a web browser (revision B GSP only). The default IP of the GSP LAN is 127.0.0.1.

NOTE The GSP has a separate LAN port from the system LAN port. It will need a separate LAN drop, IP address, and networking information from the port used by HP-UX.
Before starting this procedure, you will need to know the following information:

- I.P. address (for GSP)
- Subnet mask
- Gateway address
- Hostname (this is used when messages are logged or printed)

To configure the GSP LAN port, perform the following steps:

1. Access the GSP with the ctrl+b entry.
2. At the GSP prompt, enter the LAN Configuration (lc) command:

```
GSP> lc
```


RQS Nº 03/2005 - CN
CPMI - CORREIOS
1585
Fls:
3701
Doc:

The lc command will start a series of prompts. Respond to each prompt with the appropriate information.

Example 4-2 LC command

```
Leaving Console Mode - you may lose write access. When Console Mode returns, type
^Ecf to get console write access.

GSP Host Name:  fesrhapgsp

GSP> lc

LC This command allows you to modify the LAN configuration.

Current configuration:

MAC Address: 0x00306e050a63

IP Address: 15.8.133.185

GSP Host Name: fesrhapgsp

Subnet Mask: 255.255.248.0

Gateway: 15.8.128.1

Web Console Port Number: 2023

Do you want to modify the LAN configuration? (Y/[N])

GSP Host Name:  fesrhapgsp
```

The revision B GSP introduces a configurable Web Console Port Number parameter. The default value is 2023. Once the GSP LAN is configured, it is accessible via either TelNet or web connections.

Configuring the GSP LAN Port via LAN

The revision B GSP LAN port can be assigned an IP address without using the LAN Configuration (lc) command via an ASCII console. This section describes how to assign the IP address allowing web access. Once web access is accomplished, use the lc command to configure remaining network parameters.

NOTE The GSP LAN port is separate from the system LAN port. It will need a separate LAN drop, IP address, and networking information from the port used by HP-UX.
Before starting this procedure, you will need to know the following information:

- I.P. address (for GSP)
- Subnet mask
- Gateway address
- Hostname (this is used when messages are logged or printed)

To configure the GSP LAN port via LAN, perform the following steps:

NOTE The GSP *must* be on the same subnet as the system being used to remotely configure the LAN port. If it is not, the remote configuration will be unsuccessful.

Step 6. Determine the MAC address of the revision B GSP by examining the GSP MAC address label on the rear of the server.

Step 7. Use the `route add` command to add the I.P address of the GSP and remote system to the router.

Step 8. Use the arp command to add an ARP entry for the IP address using the GSP MAC address.

- For HP-UX systems, the format of the MAC address is 00:30:6e:05:0a:ea
- For MS DOS systems, the format of the MAC address is 00-30-6e-05-0a-ea

Step 9. Use the ping command to assign the I.P address for the GSP.

Step 10. The revision B GSP is now accessible via LAN. Access the GSP and configure remaining network parameters using the LAN Configuration (lc) command:

```
GSP> lc
```

The lc command will start a series of prompts. Respond to each prompt with the appropriate information.

Example 4-3 LAN Configuration from a PC

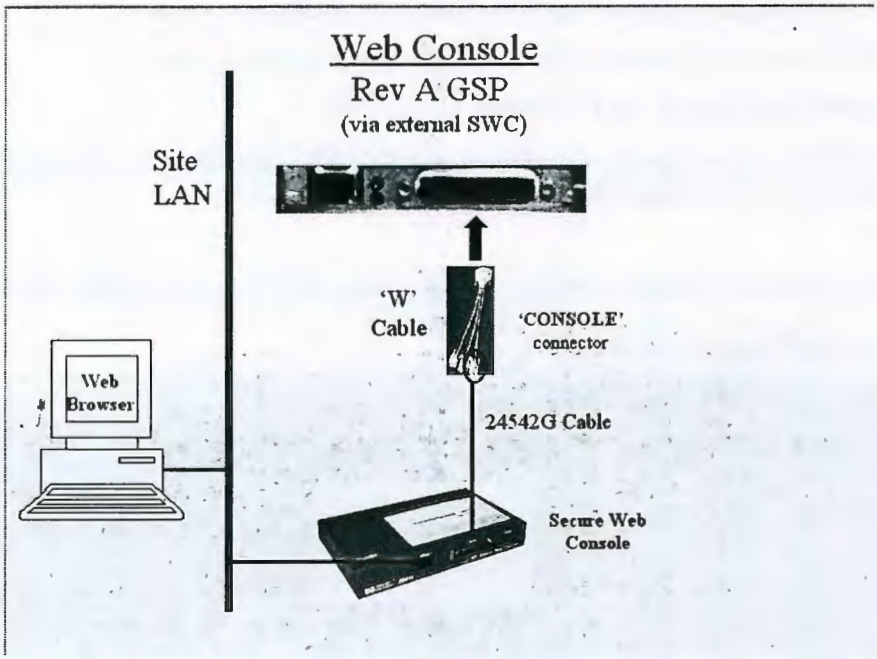
```
Command Prompt
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-1999 Microsoft Corp.

C:\>route add 15.8.130.1 15.8.133.147

C:\>arp -s 15.8.130.1 00-30-6e-05-0a-ea

C:\>ping 15.8.130.1

Pinging 15.8.130.1 with 32 bytes of data:

Reply from 15.8.130.1: bytes=32 time<10ms TTL=63
Reply from 15.8.130.1: bytes=32 time<10ms TTL=63
Reply from 15.8.130.1: bytes=32 time<10ms TTL=63
Reply from 15.8.130.1: bytes=32 time<10ms TTL=63

Ping statistics for 15.8.130.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum =  0ms, Average =  0ms

C:\>
```

Configure the Web Console

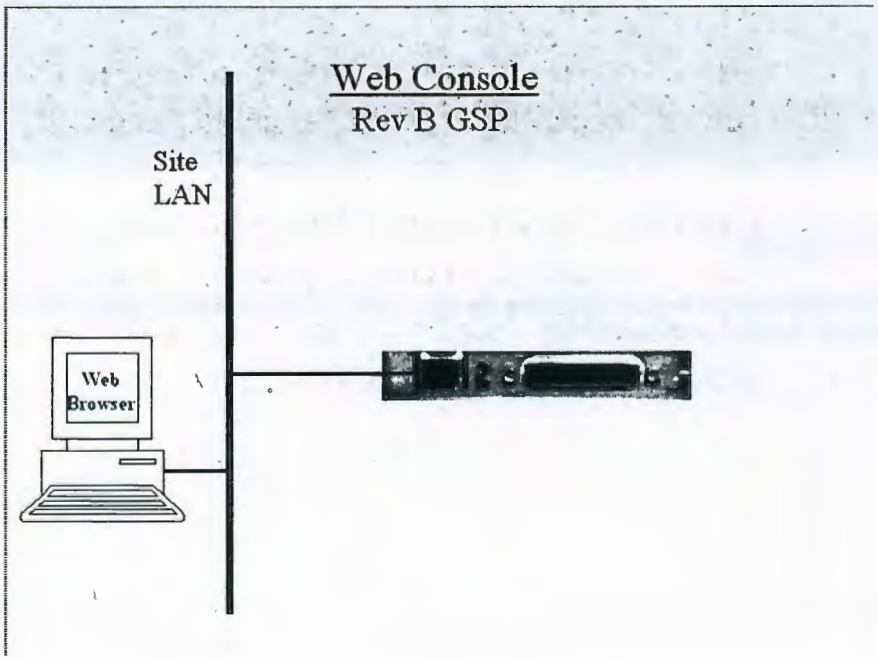
For the revision A GSP, the web console is accomplished via the J3591A Secure Web Console. Below is an illustration of the web console for the revision A GSP.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1586
Fls:
Doc: 3701

Refer to, "Install a Secure Web Console" for more information on Secure Web Console installation and configuration.



For the revision B GSP, the web console is an embedded feature. The steps to configure a web console are the same as configuring a LAN console. Refer to, "Configure the LAN Console."

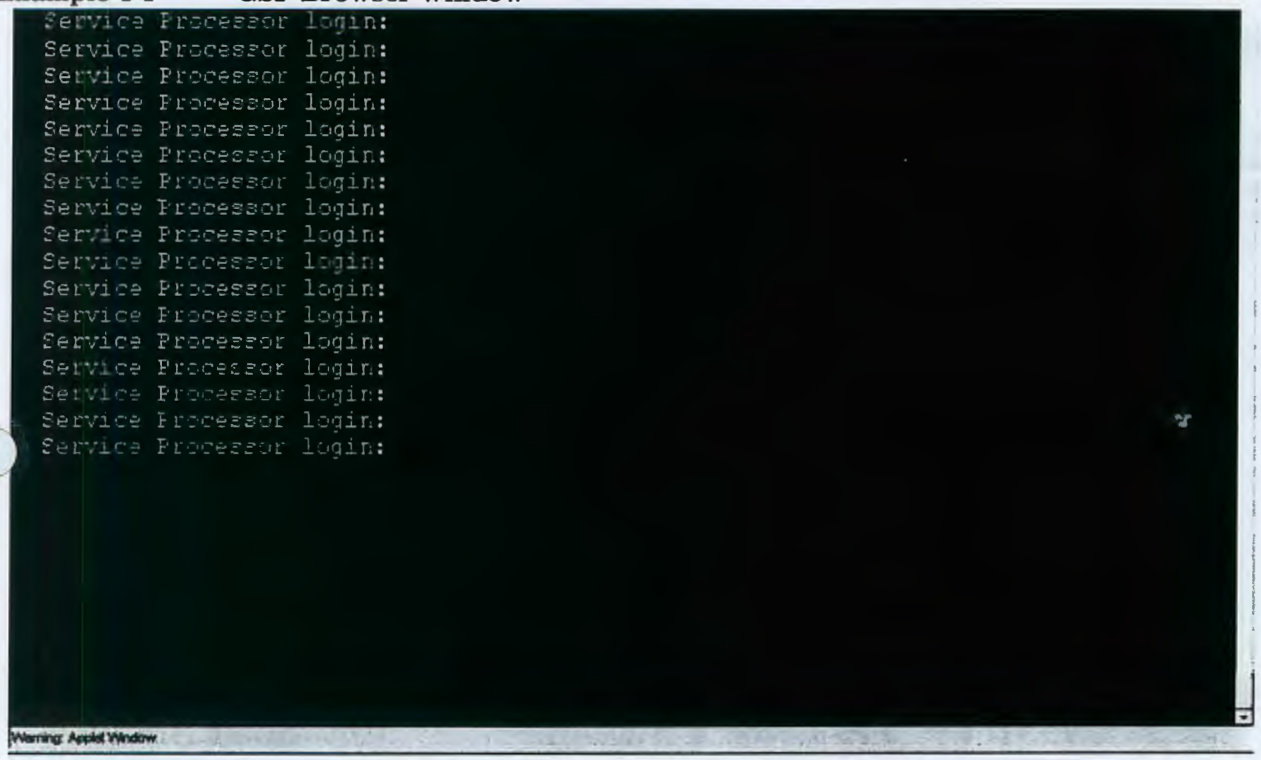


Once the LAN has been configured, access the web console by pointing a web browser, on the same subnet, to the IP of the GSP LAN.

ECT
4.767
J
PL - AC

Two browser windows will appear: a window with a white background and the HP invent logo and a separate GSP window with a black background.

Example 4-4 GSP Browser Window



Use the SETTINGS menu bar to configure web browser emulation. The GSP window also has its own HELP facility.

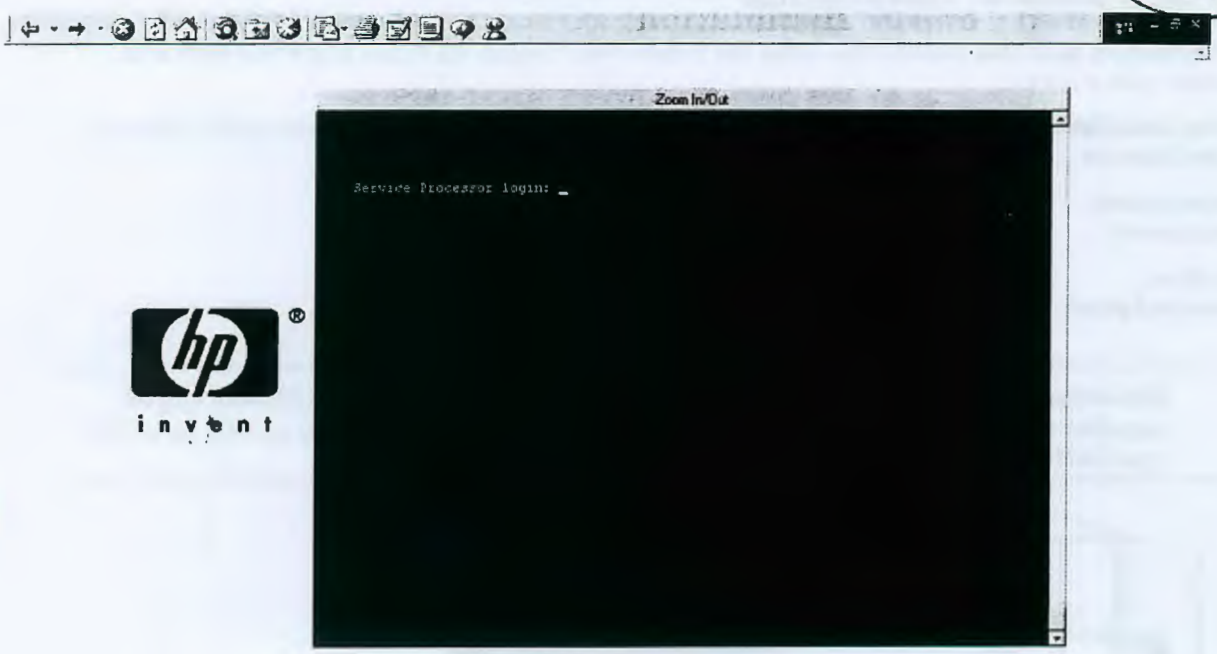
RQS Nº 03/2005 - CN
CPMI - CORREIOS
1587
Fls:
Doc: 3701

Example 4-5 GSP Web Browser Help Screen

When the separate GSP window is closed, it appears in the HP invent window with Zoom In/Out above it. Click on the Zoom In/Out bar to generate a separate GSP window.

E C T
Cable Connections
Configure System Consoles
4.765
L - AC

Example 4-6 Combined GSP Browser Window



There is not a separate administration "layer" when using the embedded web access of the revision B GSP. Web console access via the external Secure Web Console required that you first logon to the SWC, then click on ACCESS CONSOLE. User configuration was also performed at the Secure Web Console. However, the revision B GSP web console does not require this additional step. When you point the web browser at the IP of the GSP LAN, you are directly connected to the GSP. The web console part of the GSP employs the same users as the GSP.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1588
Fls: 3701
Doc:

Secure Web Console Installation

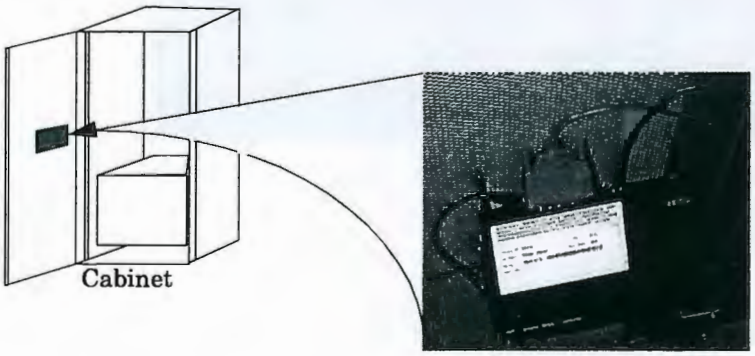
The following section describes installation of the HP Secure Web Console on inside of the rear door of a rack-mounted rp54xx server.

For technical, installation, and configuration instructions for the Secure Web Console, refer to the following URLs on the Internet:

General information:
http://www.hp.com/

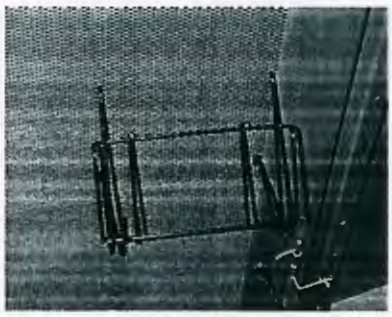
Documentation:
http://www.docs.hp.com

NOTE Either the system console (HP series 700 terminal) or the HP Secure Web Console may be installed on an rp54xx server, but not at the same time. Both console types use the same DB9 type LAN *Console* connector.



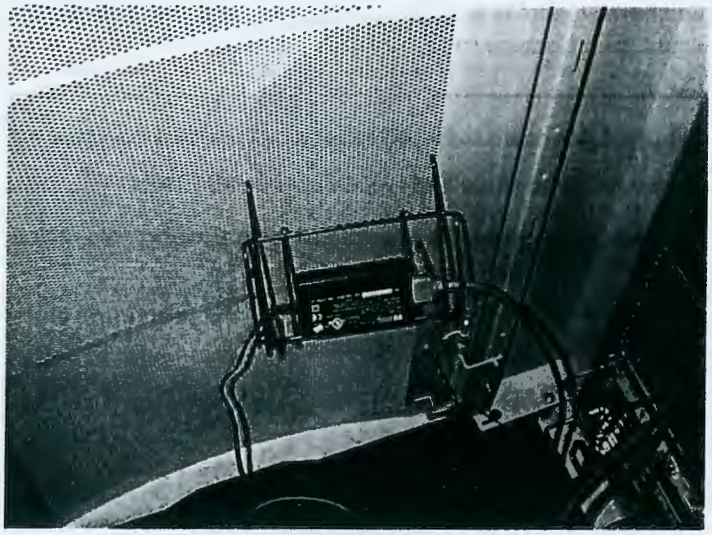
To install the HP Secure Web Console on an rp54xx server, refer to the previous figure and the HP Secure Web Console documentation, then proceed as follows:

Step 1. Install the wire mounting bracket by carefully inserting the two top prongs through the vent grill in the rear door of the cabinet as shown above. Position the bracket toward the hinge side of the door.



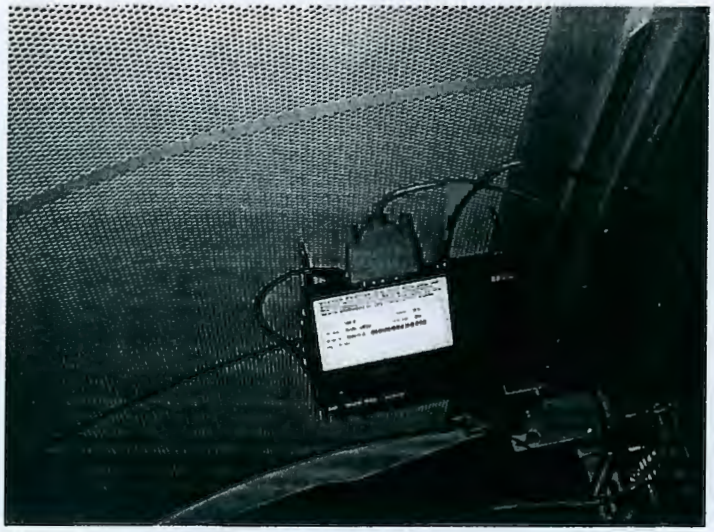
4.763
AC

Step 2. Place the Secure Web Console power supply into the bottom portion of the wire mounting bracket as shown.



Step 3. Connect one end of the power cable to the power supply where indicated.

Step 4. Position the Secure Web Console unit in the mounting bracket.



Step 5. Connect the DC out cable from the power supply to the Secure Web Console.

Step 6. Connect one end of the AC power cord (supplied) to the Secure Web Console power supply.

Step 7. Connect the other end of the AC power cord to an available receptacle.
On a PDU if in a cabinet.
In an available wall outlet if in a Deskside enclosure.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1589
Fls:
3701
Doc:

Step 8. Connect the 9-pin end of the RS-232 cable (Supplied) to the connector labeled CONSOLE on the A5591-63002 "W-type" adapter cable.

CAUTION To prevent unauthorized access to your rp54xx system, do not connect the other end of the serial cable to the Secure Web Console until both the server and the Web Console have both been fully configured.

Step 9. Connect one end of a LAN cable to RJ-45 connector labeled 10-Base-T on the Secure Web Console.

Step 10. Connect the other end of the same LAN cable to your site LAN.

Step 11. Configure the Secure Web Console in accordance with the documentation that was provided with it or refer to http://www.docs.hp.com

Step 12. Once the Web Console has been properly configured, the remaining end of the serial cable between the server and the Web Console may be connected.

E C T
4.761
L - AC

GSP Configurable Parameters

Once a system console is configured, additional GSP parameters may be set. For a complete list use the GSP>he command to access the on-line help facility.

Examples of three configurable parameters follow.

Adding Users

The GSP provides a maximum of 20 users (one administrator and 19 operators). By design, the first user added to the GSP becomes the GSP administrator. Only the GSP administrator can add or remove users or change the GSP configuration.

NOTE Before starting this procedure, you will need to know the following information:

- User's name
- Organization's name
- Login name
- User's password

To add a user, perform the following steps:

1. Access the GSP with the ctrl+b entry.
2. At the GSP prompt, enter the Security options and access control (SO) command:

   GSP> so

3. The first prompt you will see with the so command is for GSP wide parameters:

```
GSP wide parameters are:
Login Timeout: 1 minutes.
. Number of password Faults allowed: 3
. Flow Control Timeout: 5 minutes.
Do you want to modify the GSP wide parameters? (Y / [N]) __
```

   At this point you can modify the GSP wide parameters, or continue with adding users. To add users, respond N for no.

NOTE If this is the first time users are being added, the first user added will be the GSP administrator.

If this is not the first time you are adding users (you are adding additional users), you will need to step through all current users to reach the next available user prompt.

---

4. The next prompt that appears will ask the following question:

   Do you want to modify the user number 1 parameters? (Y/[N]/Q to quit) __

   Follow the series of prompts to enter all the required fields for adding a user.

RQS Nº 03/2005 - CN
CPML - CORREIOS
1590
Fls:
3791
Doc:

CAUTION Be sure to read each prompt carefully and enter the correct response. A missed or incorrect entry could deny entry to that user.

The following is an example of an added user's information:

```
. User's Name: Joe Smith
. Organization's Name: IT Support
. Dial-back configuration: Disabled
. Access Level: Operator
. Mode: multiple
. User's state: enabled
```

For the number 1 user, the Access level is administrator. The Mode entry of single only allows entry for that user one time, then access will be denied. A Mode entry of multiple allows unlimited entries into the GSP.

Removing Users

You can remove (disable) a GSP user with the same Security options and access control (SO) command used to add a user.

To remove a user, perform the following steps:

1. Access the GSP with the ctrl+b entry.
2. At the GSP prompt, enter the Security options and access control (SO) command:

   ```
   GSP> so
   ```

3. The first prompt you will see with the SO command is for GSP-wide parameters:

   ```
   GSP wide parameters are:
   . Login Timeout: 1 minutes.
   . Number of password Faults allowed: 3
   . Flow Control Timeout: 5 minutes.

   Do you want to modify the GSP wide parameters? (Y / [N]) __
   ```

   At this point you can modify the GSP wide parameters, or continue with removing a user. To remove users, respond N for no.

NOTE You will have to step through each user number until you reach the user to be removed.

4. When you access the number of the user to be removed, you must change the data in the prompts for that number.

   It is important that, at a minimum, you need to modify the User's state to Disabled.

4.759

Return the GSP to Default Configurations

The Default Configuration (dc) command is used to reset all or some of the GSP values to the default values. To return GSP values to default configurations, perform the following steps:

1. Access the GSP with the ctrl+b entry.
2. At the GSP prompt, enter the Default Configuration (dc) command:

   ```
   GSP> dc
   ```

3. Follow the prompts for the dc command, and be sure to have the change information available.

CAUTION When the Security configuration is reset, all users are removed, including the GSP administrator. It also disables the remote. Remote must be re-enabled through the main console using the Enable Remote (er) command.

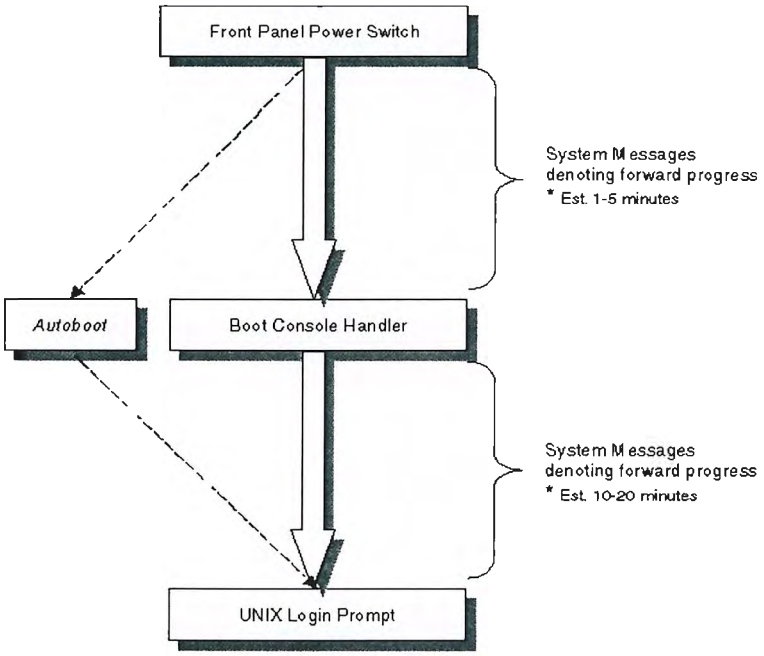
RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1591
Doc: 3701

rp54xx Server Boot Process

The length of time an rp54xx server will require to complete the boot process depends on the number of processors and the amount of RAM installed. Average configurations can take more than 20 minutes.

The boot process consists of the following main steps:

Typical Boot Process



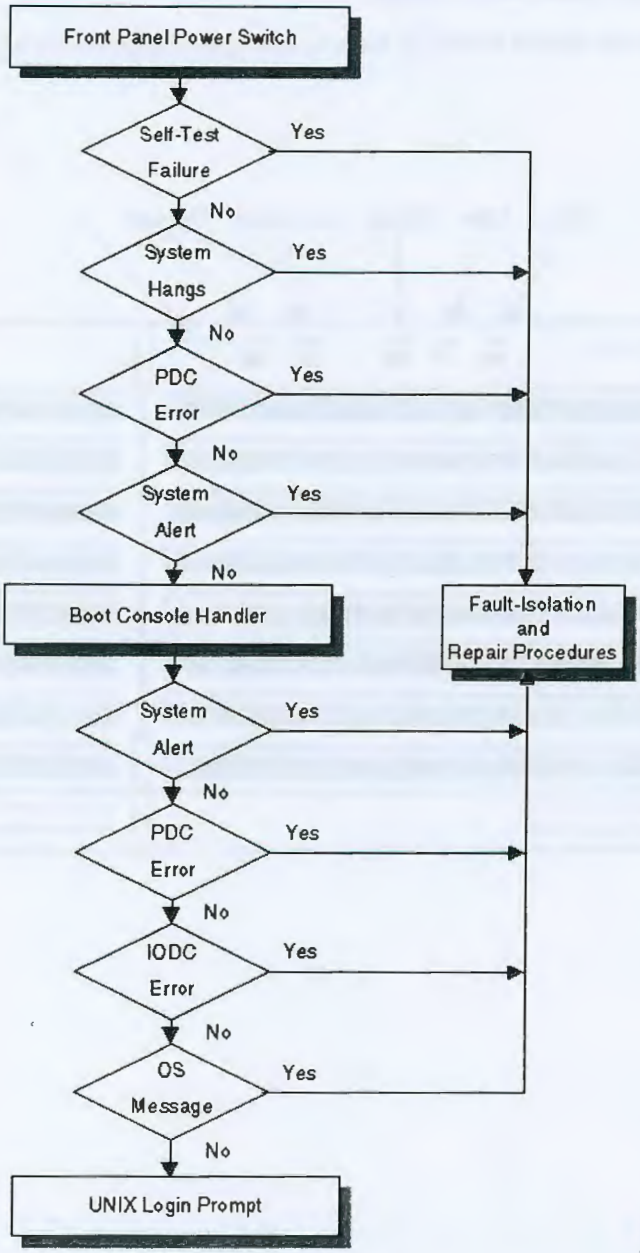
The duration of the full boot process can vary depending on:
- Number of CPUs installed
- Amount of memory installed
- UNIX version installed
- State of the network

All times approximate

E C T
4.757
J 1
A C

During the Boot process a variety of errors or problems can occur as shown below:

Potential Boot Problems



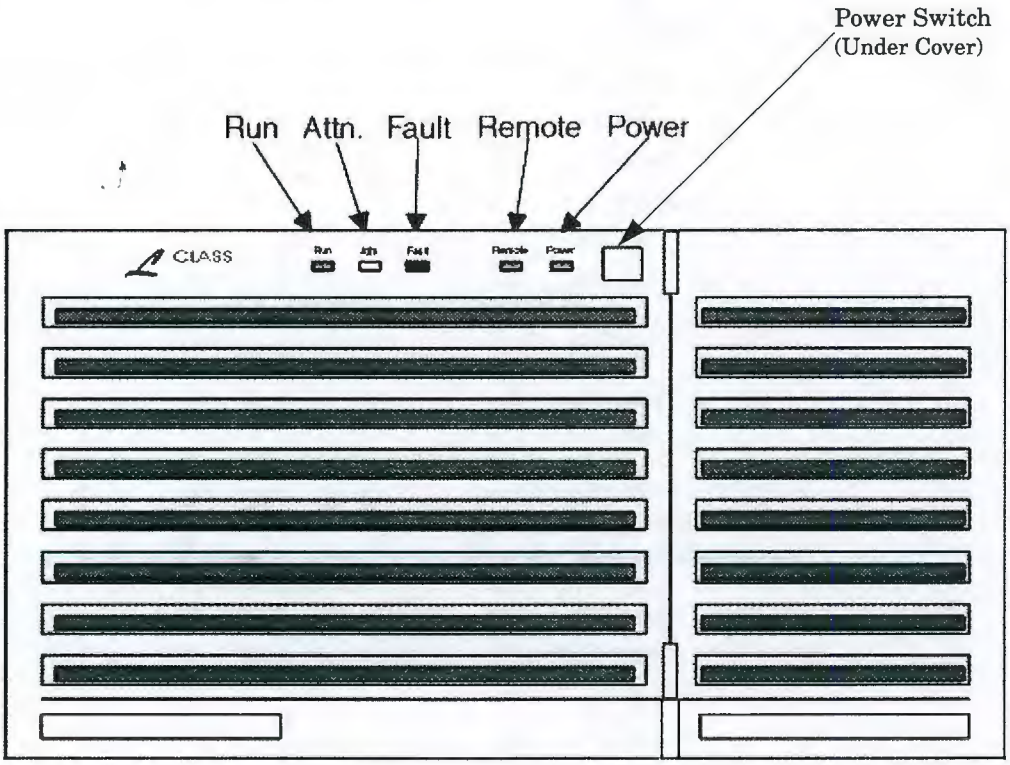
RQS Nº 03/2005 - CN
CPMI - CORREIOS
1592
Fls:
Doc: 3781

Initial Power-up

The following section describes the process of applying power to the rp54xx server and booting the system to the UNIX Login prompt. The amount of time it takes to go through self-test then boot the system will vary widely depending on hardware configuration. The following provides a "typical" procedure. Yours may vary depending on software and hardware installed:

Step 1. Apply AC Power to the system console.

Step 2. Apply power to the rp54xx server by turning the front panel switch to ON.



ECT 4.766 1 8

HotSwap Chassis Fan Replacement

The power to the server does not have to be off to remove or replace a HotSwap Chassis fan. Fan number 0 is located in the front of the server and fan number 1 is located at the rear of the server.

To replace a fan, perform the following steps:

1. Orient the fan assembly to ensure that the chassis outlet connects with the fan assembly. If the fan power connector is covered by the protective cover (see item 1 in the graphic), slide it down to remove it and slide it over the power connection on the other side of the fan. Push the fan firmly into the housing. The fan assembly will plug into the electrical outlet automatically.
2. Check the LED located on the fan.
   - When the fan is functioning normally, the LED is OFF.
   - When the fan fails, the LED is ON.

NOTE when one fan has failed (or is removed from the server), the system automatically puts the remaining fan into high speed mode. The noise level of the server will increase.

3. Replace the HotSwap Chassis fan cover.

The following graphic shows a HotSwap Chassis Fan.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1593
Fls:
Doc: 3701 155

HotSwap Card Cage Fan Removal

The power to the server does not have to be off to remove or replace a HotSwap Card Cage fan. Fans numbered 2, 3, 4, and 5 are located in a four-fan assembly housing located on the left side of the server's side service bay.

CAUTION Running the server for extended periods of time with a cooling fan removed may create hot spots inside the server and shorten component life.

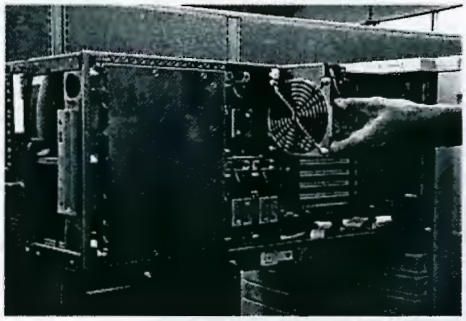
If other fans fail when one fan is removed, the system will halt.

To remove a fan from the server, perform the following step:

Identify the fan to be removed and pull it out of the Side Fan Assembly Housing. It will automatically disconnect from its electrical outlet on the I/O Backplane.

NOTE When one fan has failed (or is removed from the server) during operation, the system automatically puts the remaining fans into high speed mode. The noise level of the server will increase.

The following graphic shows a card cage fan being removed/replaced.



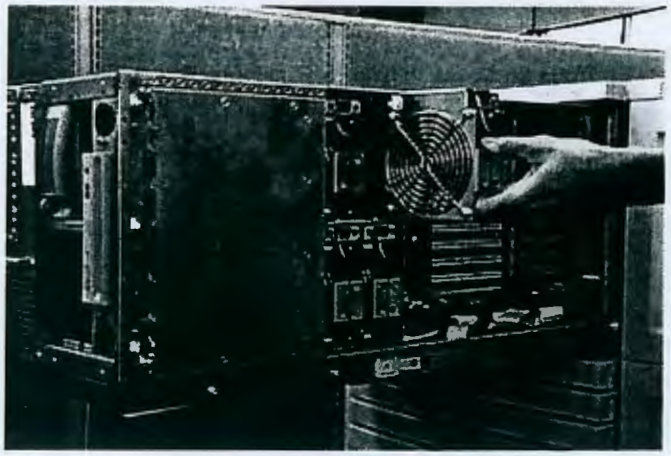
DEC
4.764
CPMI - CAC

HotSwap Card Cage Fan Replacement

The power to the server does not have to be off to remove or replace a HotSwap Card Cage fan. Fans numbered 2, 3, 4, and 5 are located in a four-fan assembly housing located on the left side of the server's side service bay.

To replace a fan in the server, orient the replacement fan into its slot in the Side Fan Assembly Housing and carefully push it in until it connects with its electrical outlet on the I/O Backplane.

The following graphic shows a card cage fan being removed/replaced.



ROS Nº 03/2005 - CN
CPMI - CORREIOS
1594
Fls:
3701
Doc: 157

HotSwap Power Supply Removal

Up to three power supplies (0 through 2), located across the bottom front of the server, can be installed in the server without removing power.

To remove a power supply from the server, perform the following step:

1. Remove the T-15 mounting screw located to the right of the handle near the top of the power supply.

CAUTION Be careful when pulling the power supply out of the server. It is heavier than it appears.

2. Grasp the handle and pull the power supply out of the server.

The following graphic shows a front and rear view of a HotSwap Power Supply.

4.755 1

Step 3. Several self-test boot progress screens will be displayed and will scroll rapidly up the screen. Some tests may pause for up to one minute while the test completes.
The following examples of the forward progress screens are typical of the screens displayed.

Brief

```
********************************* EARLY BOOT VFP ******************************

0x0000180089002380 00000000 00000000

Q/q: quit Virtual Front Panel Display
->Choice:
*******************************************************************************
```

Verbose

```
********************************* EARLY BOOT VFP ******************************
ALERT LEVEL: 0=No failure detected, forward progress
PROBLEM DETAIL: 0=no problem detail - SOURCE ID: 00
SYSTEM NAME: fespre2sas
MODEL NAME:   MODEL STRING:   S/N:
SPU POWER: ON
ACTIVITY/COMPLETION LEVEL:  0%
SYSTEM BOOT IS PENDING

LEDs:  RUN      ATTENTION     FAULT     REMOTE
       FLASH    FLASH         OFF       ON

CALLER ACTIVITY: 1=test - CALLER SUBACTIVITY: A4=implementation dependent
REPORTING ENTITY TYPE: 0=system firmware - REPORTING ENTITY ID: 01
SOURCE: 7=memory - SOURCE DETAIL: 0=unknown, no source stated

0x7800180070001A42 00000000 00000001 - type 15 = Activity Level/Timeout

Q/q: quit Virtual Front Panel Display
->Choice:
*******************************************************************************
```

RQS Nº 03/2005 - CN
GPMI - CORREIOS
1595
Fls:
3701
Doc: 75

Step 4. When the initial power-up boot process completes in approximately one to five minutes, the BCH main menu will be displayed:

```
---- Main Menu ---------------------------------------------------------------

     Command                            Description
     -------                            -----------
     BOot [PRI|ALT|<path>]              Boot from specified path
     PAth [PRI|ALT|CON|KEY] [<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
     DeBug menu                         Displays debug 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 5. To start the boot process using the primary boot path, enter *BO PRI*, at Boot Console Handler BCH main menu prompt and press **<ENTER>**.

NOTE Booting a system to a UNIX login prompt from BCH main menu can take 20 minutes or longer depending on your software and hardware configuration.

Step 6. Once the system reaches the UNIX login prompt the following will be displayed on the console screen:.

```
HP-UX hprfes A.09.04 U 9000/897 (ttyp2)

login:
```

E C T
4.753
J
C.P.L. - AC

5 Utilities

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1596
Fls:
3701
Doc:

Configuring the Rev A Guardian Service Processor (GSP)

The Rev A Guardian Service Processor (GSP) is a resident processor within the system that allows the local or remote system administrator to monitor and perform administrator functions. This section provides configuration procedures that will instruct you to:

- Configure the LAN port
- Add or delete users (maximum of 20)
- Change the default GSP configuration

Go to the appropriate section for the task that you wish to accomplish.

Configuring the GSP LAN Port

Perform the LAN configuration from the systems local port (either console or the HP secure web console).

NOTE The GSP has a separate LAN port from the system LAN port. It will need a separate LAN drop, IP address, and networking information from the port used by HP-UX.
Before starting this procedure, you will need to know the following information:

- I.P. address (for GSP)
- Subnet mask
- Gateway address
- Hostname (this is used when messages are logged or printed).

To configure the GSP LAN port, perform the following steps:

1. Go into the GSP with the ctrl+b entry.
2. At the GSP prompt, enter the LAN Configuration (lc) command:

```
GSP> lc
```

The lc command will start a series of prompts. Respond to each prompt with the appropriate information.

Adding Users

The GSP can only have a maximum of 20 users (one administrator and 19 operators). By design, the first user added to the GSP becomes the GSP administrator. Only the GSP administrator can add or remove users or change the GSP configuration.

NOTE Before starting this procedure, you will need to know the following information:

- User's name
- Organization's name
- Login name
- User's password

ECT Utilities 4-751 2 CPL - AC

To add a user, perform the following steps:

1. Enter the GSP with the ctrl+b entry.
2. At the GSP prompt, enter the Security options and access control (SO) command:

   GSP> so

3. The first prompt you see with the so command is for GSP-wide parameters:

```
GSP wide parameters are:
Login Timeout: 1 minutes.
. Number of password Faults allowed: 3
. Flow Control Timeout: 5 minutes.
Do you want to modify the GSP wide parameters? (Y / [N]) __
```

   At this point you can modify the GSP-wide parameters or continue adding users. To add users, enter N for no.

NOTE If this is the first time users are being added, the first user added will be the GSP administrator.

If this is not the first time you are adding users (you are adding additional users), you will need to step through all current users to reach the next available user prompt.

4. The next prompt that appears will ask the following question:

   Do you want to modify the user number 1 parameters? (Y/[N]/Q to quit) __

   Follow the series of prompts to enter all the required fields for adding a user.

CAUTION Be sure to read each prompt carefully and enter the correct response. A missed or incorrect entry will deny entry to that user.

The following is an example of an added users information:

```
. User's Name: Joe Smith
. Organization's Name: IT Support
. Dial-back configuration: Disabled
. Access Level: Operator
. Mode: multiple
. User's state: enabled
```

For the number 1 user, the Access level is administrator. The Mode entry of single only allows entry for that user one time, then access will be denied. A Mode entry of multiple allows unlimited entries into the GSP.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1597
Fls: 3701
Doc:

Removing Users

You can remove (disable) a GSP user with the same Security options and access control (SO) command used to add a user.

To remove a user, perform the following steps:

1. Enter the GSP with the ctrl+b entry.
2. At the GSP prompt, enter the Security options and access control (SO) command:

   ```
   GSP> so
   ```

3. The first prompt you see with the so command is for GSP-wide parameters:

   ```
   GSP wide parameters are:
   . Login Timeout: 1 minutes.
   . Number of password Faults allowed: 3
   . Flow Control Timeout: 5 minutes.

   Do you want to modify the GSP wide parameters? (Y / [N]) __
   ```

   At this point you can modify the GSP-wide parameters, or continue with removing a user. To remove users, enter N for no.

NOTE You must step through each user number until you reach the user to be removed.

---

4. When you access the number of the user to be removed, you must change the data in the prompts for that number.

   It is necessary that, at a minimum, you modify the User's state to Disabled.

Changing the Default GSP Configuration

This section describes the process of changing GSP default configurations. To change the GSP default configuration, perform the following steps:

1. Enter the GSP with the ctrl+b entry.
2. At the GSP prompt, enter the Default Configuration (dc) command:

   ```
   GSP> dc
   ```

3. Follow the prompts for the dc command, and have the change information available.

CAUTION When the Security configuration is reset, all users are removed, including the GSP administrator. The remote is disabled. The remote must be re-enabled through the main console using the Enable Remote (er) command.

E C T
4.749
CPL - AC

Configuring the Rev B Guardian Service Processor (GSP)

The Rev B Guardian Service Processor (GSP) is a resident processor within the system that allows the local or remote system administrator to monitor and perform administrator functions. This section provides configuration procedures that will instruct you to:

- Configure the LAN port
- Add or delete users (maximum of 20)
- Change the default GSP configuration

Go to the appropriate section for the task that you wish to accomplish.

Configuring the GSP LAN Port

Perform the LAN configuration from the systems local port (either console or the HP secure web console).

NOTE The GSP has a separate LAN port from the system LAN port. It will need a separate LAN drop, IP address, and networking information from the port used by HP-UX.
Before starting this procedure, you will need to know the following information:

- I.P. address (for GSP)
- Subnet mask
- Gateway address
- Hostname (this is used when messages are logged or printed)

To configure the GSP LAN port, perform the following steps:

1. Go into the GSP with the ctrl+b entry.
2. At the GSP prompt, enter the LAN Configuration (lc) command:

```
GSP> lc
```

The lc command will start a series of prompts. Respond to each prompt with the appropriate information.

Adding Users

The GSP can only have a maximum of 20 users (one administrator and 19 operators). By design, the first user added to the GSP becomes the GSP administrator. Only the GSP administrator can add or remove users or change the GSP configuration.

NOTE Before starting this procedure, you will need to know the following information:

- User's name
- Organization's name
- Login name
- User's password

ROS Nº 03/2005 - CN
CPMI - CORREIOS
1598
Fls:
3701
Doc:

To add a user, perform the following steps:

1. Go into the GSP with the ctrl+b entry.
2. At the GSP prompt, enter the Security options and access control (SO) command:

   GSP> so

3. The first prompt you will see with the so command is for GSP wide parameters:

```
GSP wide parameters are:
Login Timeout: 1 minutes.
. Number of password Faults allowed: 3
. Flow Control Timeout: 5 minutes.
Do you want to modify the GSP wide parameters? (Y / [N]) __
```

   At this point you can modify the GSP wide parameters, or continue with adding users. To add users, respond N for no.

NOTE If this is the first time users are being added, the first user added will be the GSP administrator.

If this is not the first time you are adding users (you are adding additional users), you will need to step through all current users to reach the next available user prompt.

4. The next prompt that appears will ask the following question:

   Do you want to modify the user number 1 parameters? (Y/[N]/Q to quit) __

   Follow the series of prompts to enter all the required fields for adding a user.

CAUTION Be sure to read each prompt carefully and enter the correct response. A missed or incorrect entry could deny entry to that user.

An example of an added users information would be:

```
. User's Name: Joe Smith
. Organization's Name: IT Support
. Dial-back configuration: Disabled
. Access Level: Operator
. Mode: multiple
. User's state: enabled
```

For the number 1 user, the Access level is administrator. The Mode entry of single only allows entry for that user one time, then access will be denied. A Mode entry of multiple allows unlimited entries into the GSP.

E C
CPL - AC
4747

Removing Users

You can removedisable) a GSP user with the same Security options and access control (SO) command used to add a user.

To remove a user, perform the following steps:

1. Go into the GSP with the ctrl+b entry.
2. At the GSP prompt, enter the Security options and access control (SO) command:

```
GSP> so
```

3. The first prompt you will see with the so command is for GSP wide parameters:

```
GSP wide parameters are:
. Login Timeout: 1 minutes.
. Number of password Faults allowed: 3
. Flow Control Timeout: 5 minutes.

Do you want to modify the GSP wide parameters? (Y / [N]) __
```

At this point you can modify the GSP wide parameters, or continue with removing a user. To remove users, respond N for no.

NOTE You will have to step through each user number until you reach the user to be removed.

---

4. When you access the number of the user to be removed, you must change the data in the prompts for that number.

   It is important that, at a minimum, you need to modify the User's state to Disabled.

Changing the Default GSP Configuration

This section describes the process of changing GSP default configurations. To change the GSP default configuration, perform the following steps:

1. Go into the GSP with the ctrl+b entry.
2. At the GSP prompt, enter the Default Configuration (dc) command:

```
GSP> dc
```

3. Follow the prompts for the dc command, and be sure to have the change information available.

CAUTION When the Security configuration is reset, all users are removed, including the GSP administrator. It also disables the remote. Remote must be re-enabled through the main console using the Enable Remote (er) command.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1599
Fls: 3701
Doc:

E C T
4.745
CPL - AC

6 Troubleshooting

RQS Nº 03/2005 - CN
CPMI - CORREIOS
85
Fls: 1600
Doc: 3701

Determine Current System State

To determine the current system state of an rp54xx server, first note the state of all LED indicators on the front panel. Processing this information using the decoders provided can greatly reduce the amount of time required to repair a suspected system fault.

The following procedure lists the tools available to aid you in determining the current system state.

Step 1. Determine if you can get a system prompt and if so, what kind of prompt.

Software System	Screen Prompt
Boot Console Handler (BCH)	`Main Menu: Enter command or menu>`
Guardian Service Processor (GSP)	`GSP>`
Initial System Loader (ISL)	`ISL>`
HP UNIX (HP-UX)	*Prompt varies depending on UNIX state*

Step 2. Decode the Run/Attention/Fault LED States.

Step 3. Decode the PCI I/O LED States.

Step 4. Decode the Fan, Power Supply, and Disk LED States.

Step 5. Decode the GSP LED States.

Step 6. Decode the LAN/SCSI LED States.

E C T
744
L.
AC

Troubleshooting and FRU identification

Once you have determined the current system state, you must troubleshoot the system to determine what the problem symptoms are and what repair actions to take.

Problem Symptoms and Repair Actions

Use this guide to assist you in repairing the system by matching the problem symptom with the appropriate troubleshooting step.

Table 6-1 Problem Symptoms and Repair Actions

Problem or Symptom	Problem Indicators	Normal Functioning Indicators	Troubleshooting Steps	Potential FRUs
No indication of Housekeeping voltage present when AC connected and power switch in Standby position.	Front Panel Power LED OFF when AC is plugged into system.	• Power switch Off. • Front Panel POWER LED should be FLASHING to indicate presence of Housekeeping voltage. • Power LED on GSP board should be lit solid green.	1. AC must be present. Check that PDU is plugged in. 2. Ensure there are 2 working power supplies (1 supply for rp5400). The LED on each supply should be lit. 3. Check for Service processor prompt (CTRL B at console).	• No AC present • Power Supplies • Power Converter • System Board • Display Board

ROS Nº 03/2005 - CN
CPMI - CORREIOS
1601
Fls:
3701
Doc:

Table 6-1 Problem Symptoms and Repair Actions (Continued)

Problem or Symptom	Problem Indicators	Normal Functioning Indicators	Troubleshooting Steps	Potential FRUs
System won't power on when Front Panel Power switch is turned on.	Front Panel Power LED stays BLINKING when Power Switch is turned on. ATTENTION LED may be FLASHING.	• Power switch On. • Power LED on SOLID.	1. Check for remote power shutdown via GSP>PC command. 2. *Check Error Chassis Logs*. Look for Error Chassis Log with a Source Detail = Low Voltage DC Power. This indicates a failure of one of the CPU Support Modules. The failing CPU support module is indicated in the Source ID field. 3. Ensure there are 2 working power supplies (1 supply for rp5400). The LED on each supply should be lit. 4. Check to see if GSP can communicate with platform monitor. Execute the following GSP command: GSP>PC You should get power monitor status information. 5. Housekeeping 1 voltage present indication. Check that platform monitor power LED is lit. 6. Platform Monitor functioning. Check platform monitor heartbeat LED is lit.	• Power Supplies • CPU Support Module • Platform Monitor • System Board

Table 6-1 Problem Symptoms and Repair Actions (Continued)

Problem or Symptom	Problem Indicators	Normal Functioning Indicators	Troubleshooting Steps	Potential FRUs
No BCH Main Menu prompt.	Front Panel RUN LED is not FLASHING. There is no forward progress chassis codes at the console. There is no BCH Main Menu prompt at the console.	• Flashing RUN LED. • Forward progress chassis codes. • BCH Main Menu prompt.	1. Check for red LED on GSP. If lit red, the problem is with the GSP. 2. Check that the console is properly connected and can communicate with the Service Processor (CTRL B should get you the SP login prompt). 3. Check Service Processor Error logs. Look for entries related to: • Processors • Processor Support Modules (known as low voltage DC supplies in chassis codes. Also known as power pods). • Memory 4. Reduce to minimum configuration and troubleshoot from there.	• Core I/O • Processors • Processor Support Modules • Memory • System Board • Console

RQS Nº 03/2005 - CN
CPMI - CORREIOS
89
1602
Fls:
370
Doc:

Table 6-1 Problem Symptoms and Repair Actions (Continued)

Problem or Symptom	Problem Indicators	Normal Functioning Indicators	Troubleshooting Steps	Potential FRUs
Can't boot to ISL.	Console messages indicating problems booting from the primary or alternate boot path.	• Console messages and prompt indicating you are at ISL.	1. Use BCH commands to verify I/O and presence of valid LIF devices. 2. Use BCH "Warn"command to determine if Boot is disabled. 3. Check for IODC tombstones. 4. Check SP chassis error logs.	• Disk Drive • Disk Media Backplane • LAN/SCSI Board • I/O Backplane
Can't boot HP-UX.	HP-UX boot error messages. RUN LED BLINKING.	• HP-UX boot messages. • HP-UX prompt. • RUN LED on SOLID.	1. Check SP chassis error logs. 2. Run ODE diagnostics.	• Processor • Disk Drive • Disk Media backplane • LAN/SCSI • Corrupt HP-UX

F. C. 1.740 C. CPL - AC

Chassis Code to FRU Decode

This is a guide to identify failing FRUs from System Alerts and Error Chassis Logs. The guide includes the following information:

- Cross-Referencing Chassis Log Errors to rp54xx FRUs
- Interpreting System Alerts
- Interpreting Service Processor Error Chassis Logs

There is a detailed interpretation of Chassis Logs and System Alerts in the *Interpreting Chassis Logs in Detail* guide.

Cross-Referencing Chassis Log Errors to rp54xx FRUs

Use the following table to identify the failing FRU from the Chassis Log information. You can also use the online Error Chassis Log-to-FRU Decoder utility.

1. Read the Chassis Log entry.
2. Match the **SOURCE, SOURCE DETAIL, SOURCE ID,** and **PROBLEM DETAIL** values (see table below) in the Chassis Log entry with the appropriate values in the table.
3. Read the table from left to right.

Use these examples to understand how to identify failing FRUs with the table:

- Power Supply Failure Example
- Processor Failure Example

Table 6-2 Chassis Log Error to FRU Decoder

Chassis Log Field Values and Descriptions from Log Entry					
Source	**Source Detail**	**Source ID**	**Problem Detail**	**FRU**	**Action to Take**
1 - Processor	Not Applicable (N/A)	N/A	N/A	Processor	From BCH Main Menu go to the Info Menu and execute the PR command to determine which processor is not functioning.
2 - Processor Cache	Not Applicable (N/A)	N/A	N/A	Processor	From BCH Main Menu go to the Info Menu and execute the PR command to determine which processor is not functioning.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1603
Fls:
3701
Doc:

Table 6-2 Chassis Log Error to FRU Decoder (Continued)

Chassis Log Field Values and Descriptions from Log Entry					
Source	**Source Detail**	**Source ID**	**Problem Detail**	**FRU**	**Action to Take**
3 - PDH	Not Applicable (N/A)	N/A	N/A	System Board	Replace the System Board.
4 - Power	1 - AC Mains	N/A	9 - Power Off	AC Power	Check that AC is being supplied to all power supplies.
4 - Power	3 - Low Voltage DC Power	CPU Support Module #	N/A	CPU Support Module	Replace the Processor Support Module (on the System Board) referenced in the Source ID.
4 - Power	4 - High Voltage DC Power	Power Supply #	N/A	Power Supply	Replace the Power Supply (in the front of the system behind the bezel) referenced in the Source ID.
6 - Platform	3 - Cabinet Fan	Fan #	N/A	Fan	Replace the Fan referenced in the Source ID.
6 - Platform	6 - Service Processor	N/A	N/A	Core I/O	The Service Processor is on the GSP I/O board. Replace the GSP
6 - Platform	7 - Power Monitor	N/A	N/A	Power Monitor	Replace Platform Monitor card.
7 - Memory	1 - Controller	N/A	N/A	System Board	Replace the System Board.
7 - Memory	4 - SIMM or DIMM	N/A	N/A	Memory DIMM	Isolate to failing DIMM using BCH (IN, ME) and ODE memory diagnostic.
8 - I/O	6 - Disk	N/A	Various Values	Disk Subsyste m	Use BCH commands and ODE diagnostics to check disk subsystem.

ECT
4-138
CPL - AC

Power Supply Failure Example

```
GSP> sl

SL

Which buffer are you interested in :
Incoming, Activity, Error, Current boot or Last boot ? (I/A/E/C/L) e
e

Do you want to set up filter options on this buffer ? (Y/[N]) n
n

Type + CR and CR to go up (back in time),
Type - CR and CR to go down (forward in time),
Type Q to escape.

Log Entry #   0 :
ALERT LEVEL: 6=Boot possible, pending failure or environmental problem - action required
REPORTING ENTITY TYPE: 2=power monitor - REPORTING ENTITY ID: 00
CALLER ACTIVITY: 4=monitor - CALLER SUBACTIVITY: 04=low voltage power supply
SOURCE: 4=power - SOURCE DETAIL: 4=high voltage DC power - SOURCE ID: 02
PROBLEM DETAIL: A=unexpected - ACTIVITY STATUS: F
Data  0 : Low=00000000 : High=00000000 - type  0 = Data Field Unused
Data  1 : Low=0F152A28 : High=00006303 - type 11 - Timestamp 04/15/1999 21:42:40
```

Problem Analysis

Step 1. Find the Source value. In this example, it is *SOURCE: 4=power*.

Use the **Power** row of the Error Chassis Log-to-FRU Decoder table.

Step 2. Find the Source Detail value. In this example, it is *SOURCE DETAIL: 4=high voltage DC power*.

Use the **High Voltage DC Power** row of the table.

Step 3. Find the Source ID value. In this example, it is *SOURCE ID: 02*.

The failing power supply is Power Supply #2.

Step 4. The Problem Detail for this row is not applicable.

Step 5. The FRU column of the table identifies the FRU as the Power Supply.

The correct action would be to replace Power Supply #2, located in the front of the system.

Processor Failure Example

```
Log Entry #   1 :
ALERT LEVEL: 6=Boot possible, pending failure or environmental problem - action required
REPORTING ENTITY TYPE: 0=system firmware - REPORTING ENTITY ID: 01
CALLER ACTIVITY: 1=test - CALLER SUBACTIVITY: 62=implementation dependent
SOURCE: 1=processor - SOURCE DETAIL: 1=processor general - SOURCE ID: 00
PROBLEM DETAIL: 3=functional failure - ACTIVITY STATUS: 0
Data  0 : Low=00000003 : High=F7000000 - type  0 = Data Field Unused
Data  1 : Low=0F160920 : High=00006303 - type 11 - Timestamp 04/15/1999 22:09:32
```

Problem Analysis

Step 1. Find the Source value. In this example, it is *SOURCE: 1=processor*.

Use the **Processor** row of the Error Chassis Log-to-FRU Decoder table.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1604
Fls:
3701
Doc:

Step 2. The Source Detail, the Source ID, and the Problem Detail values are all not applicable for the Processor row of the table.

Step 3. The FRU column of the table identifies the FRU as a failing processor.

Step 4. The Action column of the table instructs us to use the Info Menu and PR command of the BCH Main Menu to identify the failing processor.

Here is the output of Step 4 in our example:

```
Main Menu: Enter command or menu > in

---- Information Menu -------------------------------------------

     Command                    Description
     -------                    -----------
     ALL                        Display all system information
     BootINfo                   Display boot-related information
     CAche                      Display cache information
     ChipRevisions              Display revisions of major VLSI
     COprocessor                Display coprocessor information
     FRU                        Display FRU information
     FwrVersion                 Display firmware version
     IO                         Display I/O interface information
     LanAddress                 Display Core LAN station address
     MEmory                     Display memory information
     PRocessor                  Display processor information
     WArnings                  Display selftest warning messages

----
Information Menu: Enter command > pr

PROCESSOR INFORMATION

                        HVERSION  SVERSION              Processor
  Processor    Speed     Model    Model/Op  CVERSION      State
  ---------  --------  --------  --------  --------  -------------
      1      440  MHz   0x05c4    0x0491     2.  0   Active
      3      440  MHz   0x05c4    0x0491     2.  0   Stopped:Nonresponding

  Central Bus Speed (in MHz)    :          82
  Software ID (dec)             : 1635329341
  Software ID (hex)             : 0x6179253d
  Software Capability           : 0x01100000f0

Information Menu: Enter command >
```

Processor #3 is `Stopped:Nonresponding`. Replace Processor #3.

Interpreting System Alerts

System Alerts are reported to the system console when a problem is detected by the Service Processor. These alerts are stored in the Service Processor Error Logs. When this new alert is added to the log file, it will cause the front panel ATTENTION LED to blink.

E C T
Q-436
L.
A C

Interpreting System Alerts

Do one of the following:

1. No response: the alert will time out and the system will continue operating.
2. **A** - Responding with the letter **A** will inform the Service Processor that you have seen the entry. The system will continue to operate.
3. **X** - Responding with the letter **X** will inform the Service Processor to disable all future alert messages. This can be re-enabled with a Service Processor command.

Sample System Alert

```
*************************SYSTEM ALERT*************************************
ALERT LEVEL: 6=Boot possible, pending failure or environmental problem - action required
PROBLEM DETAIL: 4=fan failure - SOURCE ID: 04
SYSTEM NAME: fesrhapgsp

MODEL NAME:    MODEL STRING:    S/N:
SPU POWER: ON
ACTIVITY/COMPLETION LEVEL:  0%
SYSTEM BOOT IS PENDING

LEDs:  RUN       ATTENTION     FAULT     REMOTE
       FLASH     OFF           OFF       ON

CALLER ACTIVITY: 4=monitor - CALLER SUBACTIVITY: 05=fan
REPORTING ENTITY TYPE: 2=power monitor - REPORTING ENTITY ID: 00
SOURCE: 6=platform - SOURCE DETAIL: 3=cabinet fan

0x002008646304405F 00000000 00000000 - type  0 = Data Field Unused

0x582008646304405F 00006303 0F151D08 - type 11 = Timestamp 04/15/1999 21:29:08
A: ack read of this entry - X: Disable all future alert messages
Anything else skip redisplay the log entry
->Choice:a
```

Key FRU Identification Fields for System Alerts

The following fields are used for FRU identification.

Alert Level:	How the problem has affected the system operation.
Source:	What major part of the system the alert is referring to (i.e, platform, memory, processor, etc...).
Source Detail:	What sub-part of the system the alert is referring to (i.e, cabinet fan, DIMM, high voltage DC power, etc...).
Source ID:	Specific FRU referred to in Source and Source Detail (i.e, cabinet fan #4).
Problem Detail:	Specific problem information (i.e, power off, functional failure, etc...).
Timestamp:	When the problem occurred.

The above sample system alert shows the following:

1. The problem does not affect system boot.
2. The problem is with platform cabinet fan #4.
3. The problem is a fan failure. Replace fan #4 to correct the problem.
4. The fan failed on April 15, 1999 at 9:29 PM.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1605
Fls:
3701
Doc:

Interpreting Service Processor Error Chassis Logs

Accessing the Service Processor Error Chassis Logs will turn the **ATTENTION** LED, blinking on the front panel, OFF.

Chassis Logs (located in the Service Processor) contain low level logging information related to the following 5 categories:

- Incoming log: Contains all chassis logs coming into the Service Processor.
- Activity log: Contains all chassis logs related to system activity.
- Error log: Contains all error chassis logs.
- Current boot log: Contains all chassis logs associated with the current boot.
- Last boot log: Contains all chassis logs associated with the last boot.

The Error Chassis Logs are the ones you need to look at.

Accessing Error Chassis Logs

Execute the following steps to access the Error Chassis Logs.

1. At the system console prompt, type **CTRL B**
2. Enter the Service Processor Login and Password
3. The screen will display: GSP>

   At the GSP> prompt: type SL and press enter
4. The screen will display:

   `Which buffer are you interested in:`
   `Incoming, Error, Current boot, Last boot? (I/A/E/C/L)`, type **E**, and press enter
5. The screen will display:

   Do you want to set up filter options on this buffer? (Y/[N]), type **N**, and press enter
6. The most recent Error Log Entry (Log Entry #0) will be displayed. A carriage return after this will display the next log entry. Type Q to stop displaying the log entries. The screen will display: GSP>
7. At the GSP> prompt: type CO, and press enter to return to the console screen.

Example of Accessing Error Logs

Here is an example of accessing the Error Logs from the Boot Console Handler (BCH) Main Menu prompt. User input is shown in *ITALICS*.

```
Main Menu: Enter command or menu > type CTRL B
Service Processor login: System Operator
Service Processor password: ****** (password hidden)

            Welcome to HP Guardian Service Processor
            System Name: fesrhapgsp


fesrhapgsp:
ALERT LEVEL: 6=Boot possible, pending failure or environmental problem - action required
SOURCE: 6=platform - SOURCE DETAIL: 3=cabinet fan
PROBLEM DETAIL: 4=fan failure
GSP>
```

```
HP Guardian Service Processor Command Interface
Type HE to get the list of available commands

fesrhapgsp:
ALERT LEVEL: 6=Boot possible, pending failure or environmental problem - action required
SOURCE: 6=platform - SOURCE DETAIL: 3=cabinet fan
PROBLEM DETAIL: 4=fan failure
GSP> sl

SL

Which buffer are you interested in :
Incoming, Activity, Error, Current boot or Last boot ? (I/A/E/C/L) e
e

Do you want to set up filter options on this buffer ? (Y/[N]) n
n

Type + CR and CR to go up (back in time),
Type - CR and CR to go down (forward in time),
Type Q CR to escape.

Log Entry #   0 :
ALERT LEVEL: 6=Boot possible, pending failure or environmental problem - action required
REPORTING ENTITY TYPE: 2=power monitor - REPORTING ENTITY ID: 00
CALLER ACTIVITY: 4=monitor - CALLER SUBACTIVITY: 05=fan
SOURCE: 6=platform - SOURCE DETAIL: 3=cabinet fan - SOURCE ID: 04
PROBLEM DETAIL: 4=fan failure - ACTIVITY STATUS: F
Data  0 : Low=00000000 : High=00000000 - type  0 = Data Field Unused
Data  1 : Low=0F151D08 : High=00006303 - type 11 = Timestamp 04/15/1999 21:29:08


q

fesrhapgsp:
ALERT LEVEL: 6=Boot possible, pending failure or environmental problem - action required
SOURCE: 6=platform - SOURCE DETAIL: 3=cabinet fan
PROBLEM DETAIL: 4=fan failure
GSP> co

CO

You are now leaving the Guardian Service Processor Command Interface
and returning to the console mode.  Type Ctrl B to reactivate it.

Main Menu: Enter command or menu >
```

Key FRU Identification Fields for Error Chassis Logs

The following fields are for FRU identification.

Alert Level:	How the problem has affected the system operation.
Source:	What major part of the system the alert is referring to (i.e., platform, memory, processor, etc.).
Source Detail:	What sub-part of the system the alert is referring to (i.e., cabinet fan, DIMM, high voltage DC power, etc.).
Source ID:	Specific FRU referred to in Source and Source Detail (i.e., fan #4).
Problem Detail:	Specific problem information (i.e, power off, functional failure, etc.).
Timestamp:	When the problem occurred.

The above sample system alert message shows the following:

1. The problem does not affect booting of the system.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1606
Fls:
3701
Doc:

2. The problem is with fan #4.
3. The problem is a fan failure.
4. The fan failed on April 15, 1999 at 9:29 PM.

In this example, fan #4 should be replaced to correct the problem.

Interpreting Chassis Logs Using the chassis_code.codes File

For chassis logs generated by system firmware (Reporting Entity Type 0), use the chassis_code.codes file for chassis code definitions. Each revision of system firmware (AKA Processor Dependent Code or PDC) has a unique chassis_code.codes file. This file is not part of either the PF_Cxxxxx or PHSS_xxxxx server firmware patches. The chassis_code.codes files appear in the appendices of the *Interpreting Chassis Logs in Detail* guide.

The definition of a PDC reported chassis code is determined by locating either the last four digits of a chassis log or the last three digits of a selftest chassis code in the appropriate chassis_code.codes file. Refer to the *Interpreting Chassis Logs in Detail* guide for definition and examples of selftest chassis codes.

NOTE Be sure to use the appropriate appendix as the PDC for rp5400/rp5450 is different than PDC for rp5470. Using the wrong appendix may result in a mis-interpretation of the chassis code.

To quickly learn the definition of a PDC reported chassis code, follow these four steps:

Step 1. Determine either the last 4 digits of the hex chassis code or the last 3 digits of the selftest chassis code.

Step 2. Go to the appropriate appendix in the *Interpreting Chassis Logs in Detail* guide.

Step 3. Locate the chassis code that matches the last 3 or 4 digits. If viewing via web browser or Adobe Acrobat, use the FIND feature to locate the chassis code.

Step 4. Take action as appropriate.

ECT
CPL - AC

Example 6-1 Chassis Log: Reporting Entity Type = System Firmware

```
Log Entry #   0 :SYSTEM NAME: fesrhapgspDATE: 12/08/2000 TIME: 23:46:22ALERT LEVEL: 6
= Boot possible, pending failure - action requiredSOURCE: 3 = PDHSOURCE DETAIL: 0 =
unknown, no source stated   SOURCE ID: 3PROBLEM DETAIL: 0 = no problem detailCALLER
ACTIVITY: 1 = test   STATUS: 0CALLER SUBACTIVITY: 71 = implementation
dependentREPORTING ENTITY TYPE: 0 = system firmware   REPORTING ENTITY ID:
030x0000306030031710 00000000 000000FE type  0 = Data Field Unused0x5800386030031710
0000640B 08172E16 type 11 = Timestamp 12/08/2000 23:46:22Type CR for next entry, Q CR
to quit.
```

Using the example above:

Step 1. The last 4 digits are 1710.

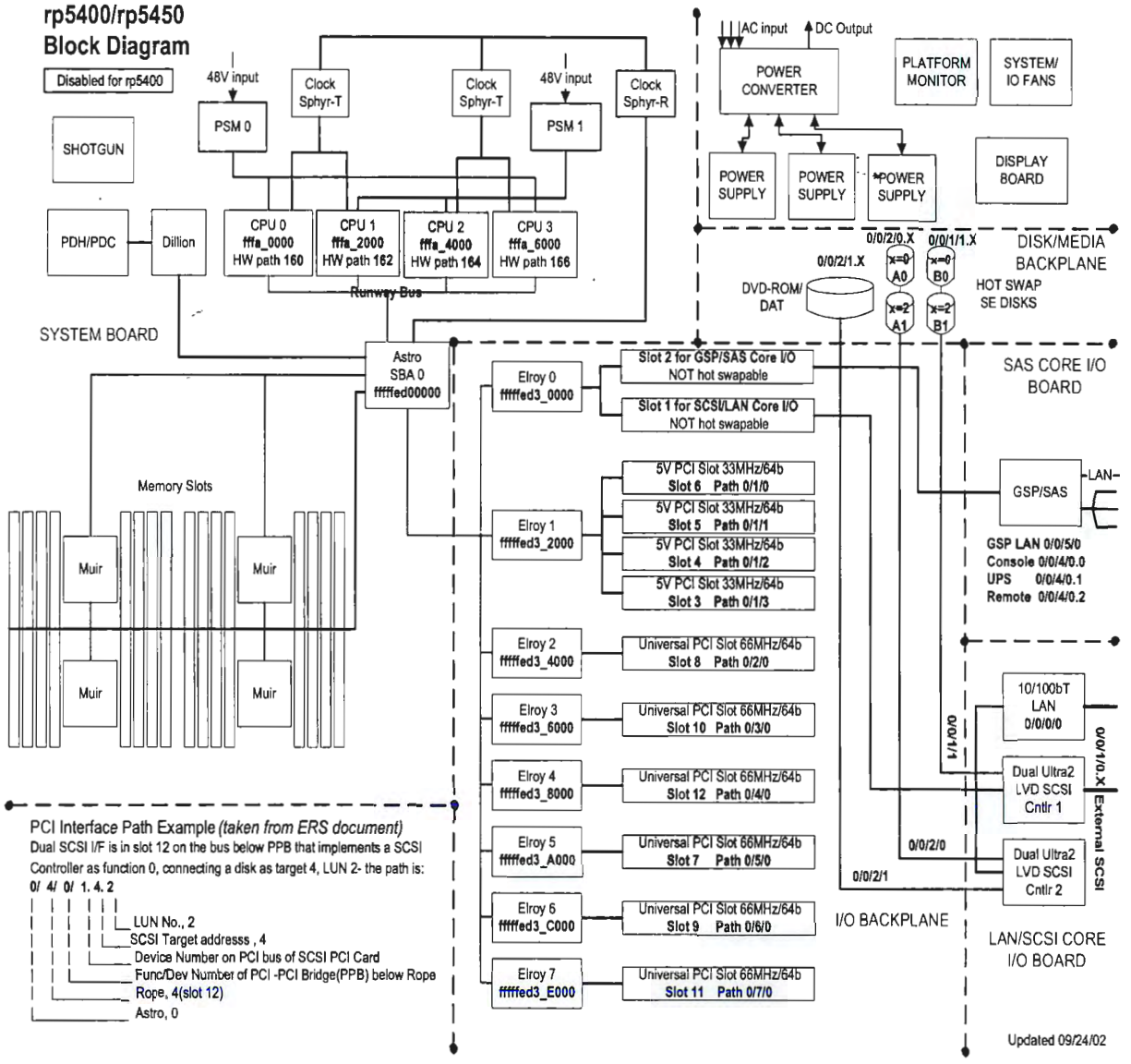
Step 2. This is an rp5450 so use Appendix B in the *Interpreting Chassis Logs in Detail* guide.

Step 3. Using the FIND feature to look up 1710 in Appendix B, we learn the definition is CC_BOOT_INVALID_SPHYR_SETTINGS.

Step 4. The appropriate action in this example would be to verify the switch settings on the system board are set correctly for the installed CPU's.

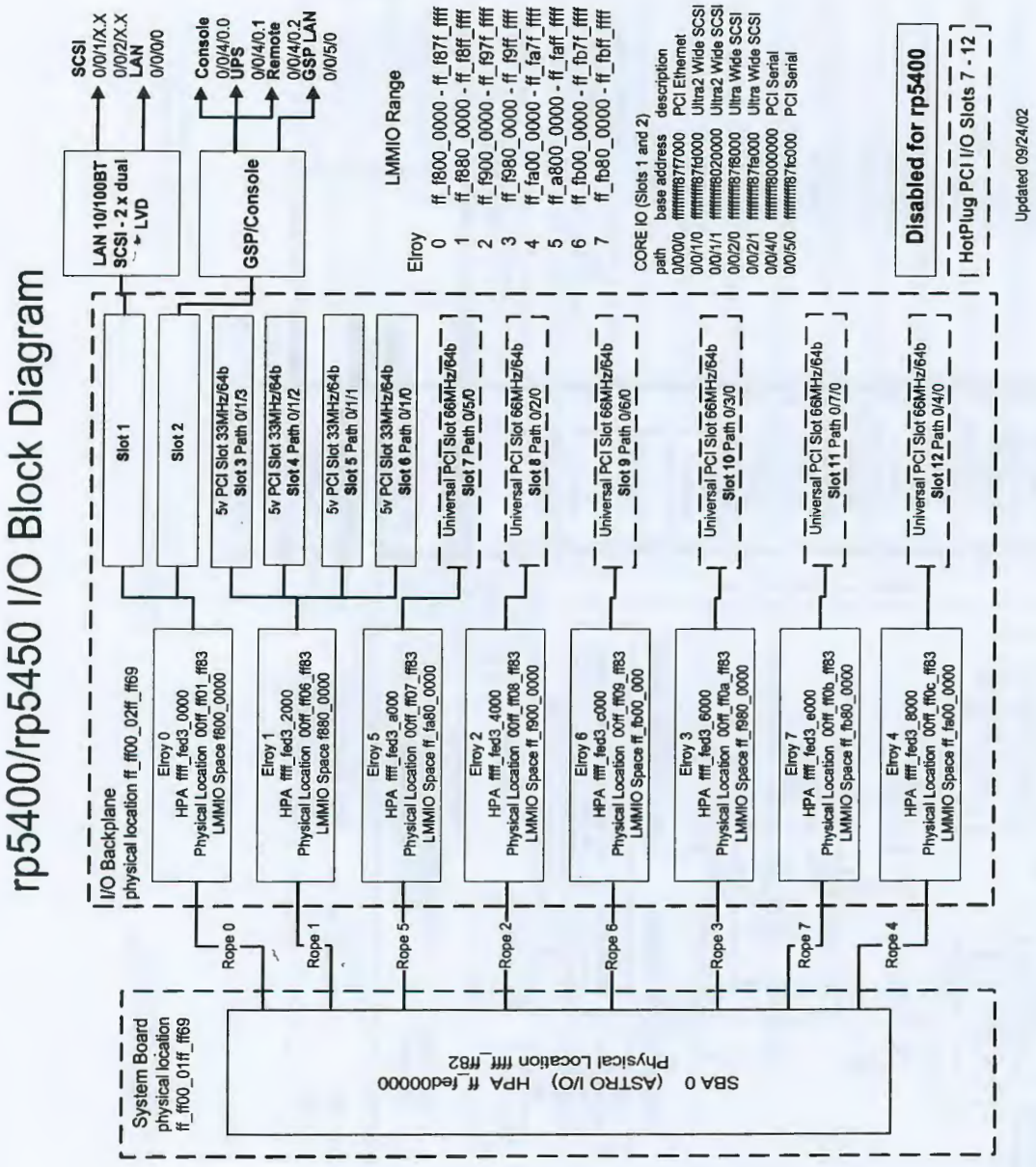
ROS Nº 03/2005 - CN
CPMI - CORREIOS
1607
Fls:
3701
Doc:

rp5400 and rp5450 System Block Diagram



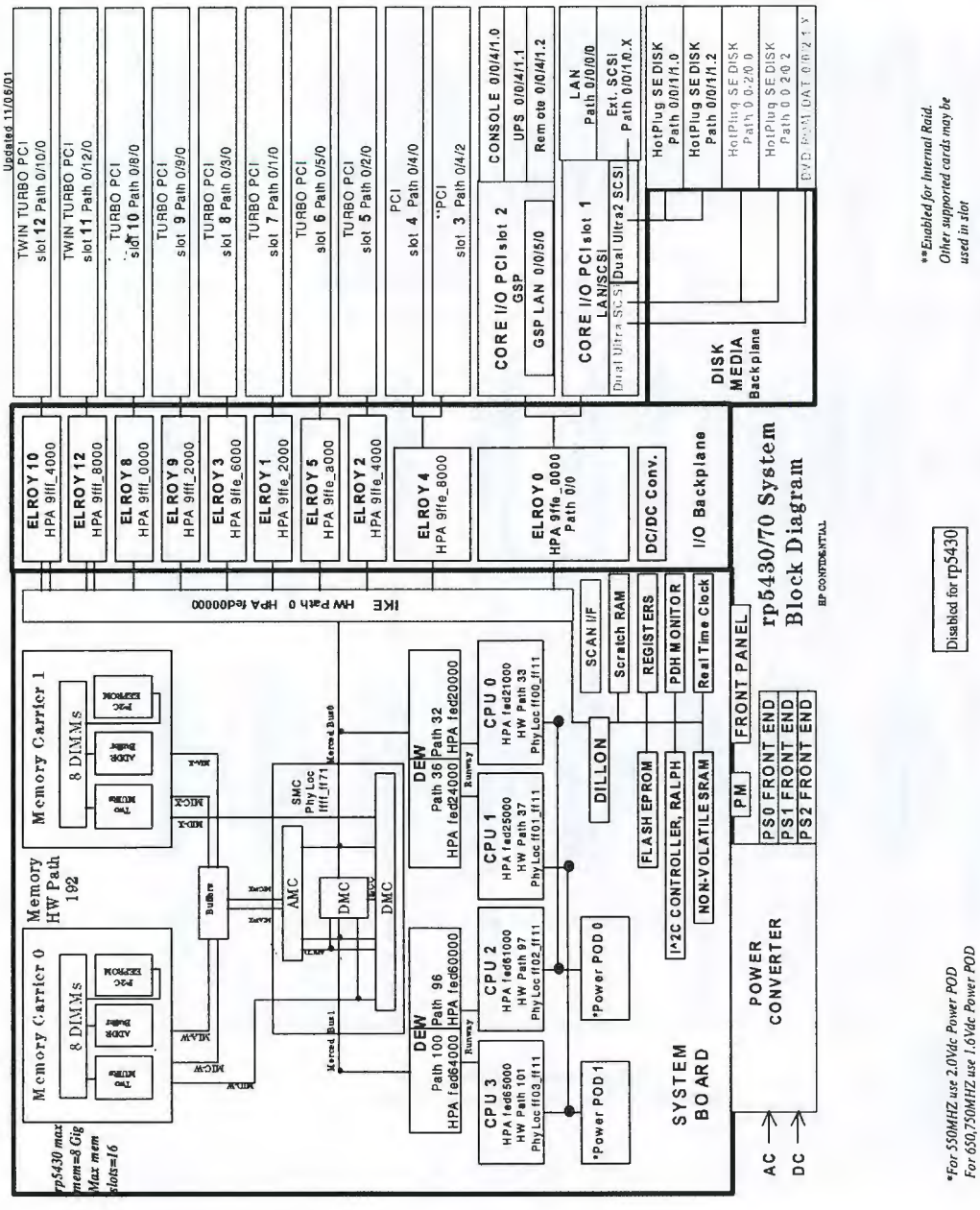
E C T
4.730
JAC

rp5400 and rp5450 I/O Block Diagram



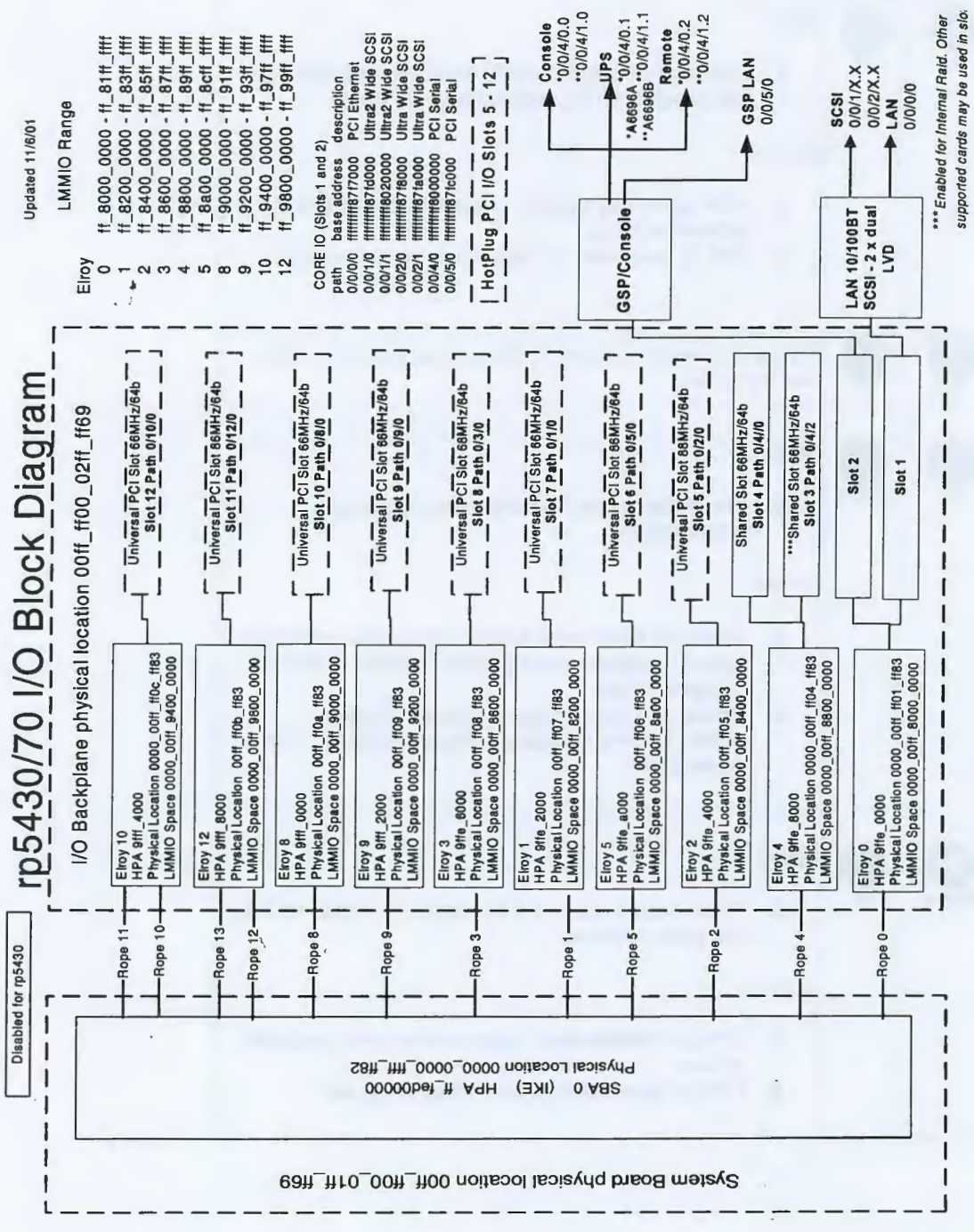
RQS Nº 03/2005 - CN
CPMI - CORREIOS
101
Fls: 1608
Doc: 3701

rp5430 and rp5470 System Block Diagram



4.728
3
AC

rp5430 and rp5470 I/O Block Diagram



RQS Nº 03/2005 - CN
CPMI - CORREIOS
103
1609
Fls:
3701
Doc:

Run/Attention/Fault LED States

Run (Green)	Attn (Amber)	Fault (Red)	Description
On	Off	Off	State: ▯ System running normally. You should expect an OS prompt, if not, system may be hung. Action: ▯ Attempt to get system prompt to determine if system is hung. ▯ Talk to customer to determine reason for call.
On	Off	On	This is an invalid indication. Check the server's LEDs and try again.
On	Off	Flashing	State: ▯ The system crashed and rebooted itself successfully Action: ▯ Check chassis error logs to determine probable cause of system crash (either HPMC or HP-UX System Panic) ▯ Check service processor console logs for potential error messages from the OS (ie. Panic messages)
On	Flashing	Off	State: ▯ There was a system interruption that did not take the system down Action: ▯ Check chassis error logs to determine probable cause ▯ Check Sentinel logs for probable cause

E C T
4.726
JAC

Run (Green)	Attn (Amber)	Fault (Red)	Description
On	Flashing	On	This is an invalid indication. Check the server's LEDs and try again.
On	Flashing	Flashing	State: ▯ System running, and ▯ A) unexpected reboot occurred, and ▯ B) a non-critical error has been detected Action: ▯ A) Check chassis error logs to determine probable cause of system crash (either HPMC or HP-UX System Panic) ▯ A) Check GSP console logs for potential error messages from the OS (ie. Panic messages) ▯ B) Check chassis error logs to determine probable cause of non-critical error ▯ B) Check Sentinel logs for probable cause of non-critical error

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1610
Fls:
3701
Doc:

Run (Green)	Attn (Amber)	Fault (Red)	Description
Flashing	Off	Off	State: ▯ Executing non-OS code - no problems detected ▯ System may be hung or waiting for BCH response ▯ Potential causes could be PDC never executed (problem with fetching code from PDH), HPMC while PDC was configuring system. Action: ▯ Check console for pending responses ▯ If system appears to be hung, execute TC from GSP prompt and check Last Boot Log for details of previous boot attempt. Pay attention to time stamps to ensure Last Boot Log reflects last boot attempt. ▯ If necessary, bring system down to minimum configuration, processors, memory, I/O, and troubleshoot.

E C T
2472
L - AC

Run (Green)	Attn (Amber)	Fault (Red)	Description
Flashing	Off	On	State: ▯ Boot failed ▯ Executing non-OS code. Action: ▯ 1. Check chassis error logs ▯ 2. Read console messages for indications of problems ie. warnings from PDC
Flashing	Off	Flashing	State: ▯ Unexpected reboot occurred ▯ Executing non-OS code. Action: ▯ 1. Check chassis error logs ▯ 2. Read console messages for indications of problems ie. warnings from PDC
Flashing	Flashing	Off	State: ▯ Executing non-OS code. ▯ Non-critical error detected (ie. fan failure, power supply failure) Action: ▯ Read chassis error logs starting at entry 0 to determine cause of flashing amber LED and fix problem.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1611
Fls:
3701
Doc:

Run (Green)	Attn (Amber)	Fault (Red)	Description
Flashing	Flashing	On	State: ▯ Boot failed ▯ Executing non-OS code. ▯ Non-critical error detected (ie. fan failure, power supply failure) Action: ▯ 1. Check chassis error logs ▯ 2. Read console messages for indications of problems ie. warnings from PDC
Flashing	Flashing	Flashing	State: ▯ Unexpected reboot/system recovering. ▯ Executing non-OS code. ▯ Non-critical error detected (ie. fan failure, power supply failure) Action: ▯ 1. Check chassis error logs ▯ 2. Read console messages for indications of problems ie. warnings from PDC

ECT
4.720
CPL - AC

Run (Green)	Attn (Amber)	Fault (Red)	Description
Off	Off	Off	State: ▯ A) If Power LED Off ▯ B) If Power LED Flashing ▯ C) If Power LED On Action: ▯ A) Check Power Supply switches and LEDs ▯ Power supply switches should be on and LEDs should be on to indicate presence of AC. If Power Supply LEDs are on and the Front Panel LED is off, replace Power Monitor. ▯ Check AC power at source ▯ B) Turn Front Panel Power Switch on - LED should be on solid ▯ If LED continues to flash, system has been remotely powered off by the service processor or the power monitor has failed. ▯ Execute service processor PC command: type CTRL B, log into the service processor, and type PC at the prompt. ▯ If this doesn't cause the LED to go on solid, problem is most likely with the power monitor. ▯ C) Cannot execute PDC. If more than one processor installed, the problem is most likely a failed system board. If only one processor installed, problem could be either the processor or system board.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1612
Fls:
3701
Doc:

Run (Green)	Attn (Amber)	Fault (Red)	Description
Off	Off	On	State: ▯ Boot failed ▯ OS not up and running, PDC has detected a failure that is preventing boot from occurring. Action: ▯ 1. Check chassis error logs ▯ 2. Read console messages for indications of problems ie. warnings from PDC
Off	Off	Flashing	This is an invalid indication. Check the server's LEDs and try again.
Off	Flashing	Off	State: ▯ No code is executing (PDC, OS or Diagnostics) ▯ Non-critical error detected (ie. fan failure, power supply failure) (Double fault situation) Action: ▯ Cannot execute PDC. If more than one processor installed, the problem is most likely a failed system board. If only one processor installed, problem could be either the processor or system board. ▯ Check chassis error logs to determine the source of non-critical error.

ECT 4.720 1 L - AC

Run (Green)	Attn (Amber)	Fault (Red)	Description
Off	Flashing	On	State: ▯ Boot failed ▯ OS not up and running, PDC has detected a failure that is preventing boot from occurring. ▯ Non-critical error detected (ie. fan failure, power supply failure) Action: ▯ 1. Check chassis logs ▯ 2. Read console messages for indications of problems ie. warnings from PDC
Off	Flashing	Flashing	This is an invalid indication. Check the server's LEDs and try again.
	On		Any combination with amber on is an invalid indication since amber is never on solid.

ROS Nº 03/2005 - CN
CPMI - CORREIOS
1613
Fls:
3701
Doc:

PCI I/O LED States

Power (green)	Attention (amber)	State
On	Off	State: ▯ Normal operation
On	On	State: ▯ Slot selected <or> slot located ▯ Power on Action: ▯ Not ready for OLRAD
Off	On	State: ▯ Slot selected <or> slot located ▯ Power is off Action: ▯ Ready for OLRAD
On	Flashing	State: ▯ Fault detected ▯ Power on

E C T
4.718
CPL - AC

Power (green)	Attention (amber)	State
Off	Flashing	State: ▯ Fault detected ▯ Power off
Off	Off	State: ▯ Slot available

ROS Nº 03/2005 - CN
CPMI - CORREIOS
113
1614
Fls:
3701
Doc:

Expansion I/O LED States

Power (green)	Attention (amber)	State
On	On	State: ▯ Slot selected <or> slot located ▯ Power on Action: ▯ Not ready for OLRAD
Power (green)	Attention (amber)	State
On	Off	State: ▯ Normal operation
Power (green)	Attention (amber)	State
On	Flashing	State: ▯ Fault detected ▯ Power on
Power (green)	Attention (amber)	State
Off	On	State: ▯ Slot selected <or> slot located ▯ Power is off Action: ▯ Ready for OLRAD

E C T
4.716
CPL - AC

Power (green)	Attention (amber)	State
Off	Off	State: ▯ Slot available
Power (green)	Attention (amber)	State
Off	Flashing	State: ▯ Fault detected ▯ Power off

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1615
Fls:
3701
Doc:

GSP LED States

GSP - Revision A

Type	Status	State
GSP Upper	On Green	State: ▯ GSP Power OK
	Flashing Green	State: ▯ GSP LAN receive
	On Red	State: ▯ GSP Failure
GSP Lower	On Green	State: ▯ Link OK
	Flashing Green	State: ▯ GSP LAN transmit
	On Red	State: ▯ GSP Failure

E C T
4.714
J
J S L - AC

GSP - Revision B

Type	Status	State
GSP Upper	On Green	State: ▯ GSP Power OK
	Flashing Green	State: ▯ GSP LAN receive
	On Red	State: ▯ GSP Failure
GSP Lower	On Amber	State: ▯ 10 Base-T Link OK
	Flashing Amber	State: ▯ 10 Base-T Activity
	On Green	State: ▯ 10 Base-T Link OK
	Flashing Green	State: ▯ 10 Base-T Activity

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1616
Fls:
Doc: 3701

LAN/SCSI LED States

Type	Status			State
LAN Upper	On Green	- or -	Flashing Green	State: ▯ 100bT Mode
	On Amber	- or -	Flashing Amber	State: ▯ 10bT Mode
LAN Lower	On Green	- or -	Flashing Green	State: ▯ LAN Transmit
SCSI Upper	On Green			State: ▯ LVD Mode
	Off			State: ▯ Single Ended Mode
SCSI Lower	On Amber			State: ▯ Termpower Present
	Off			State: ▯ Termpower Absent

E C T
4-712
P M L J - A C

Fan, Power Supply, and Disk LED States

Type	Status	State
Fan	On Amber	State: ▯ Fan Failure
	Off	State: ▯ Normal operation
Power Supply	On Green	State: ▯ Normal operation
	Off	State: ▯ Power-Supply Failure
Disk Activity	On Green or Flashing Green	State: ▯ Normal Activity
	Off	State: ▯ No Activity - Normal
Disk Attention	On Amber	State: ▯ Ready for HotPlug
	Off	State: ▯ Normal

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1617
Doc: 3701

E C T
4.710
J
L - AC

7 Removing and Replacing Components

The following list of parts can be changed when required to keep the system running properly. The remove/replace components shown under each part indicates the path required for access to each.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1613
Fls:
3701
Doc:

List of Changeable Parts with Remove and Replace Components

NOTE When viewed in PDF format, component remove/replace instructions may be accessed directly by clicking on the component title listed under each part.

Cardcage Fan

Extend the Server out the Front (If Racked)

Stand-alone Server Cover Removal (If Not Racked)

Side Cover Removal

HotSwap Card Cage Fan Removal

HotSwap Card Cage Fan Replacement

Side Cover Replacement

Stand-alone Server Cover Replacement (If Not Racked)

Insert the Server from the Front (If Racked)

Core I/O

Extend the Server out the Front (If Racked)

Stand-alone Server Cover Removal (If Not Racked)

Side Cover Removal

Core I/O Removal

Core I/O Replacement

Side Cover Replacement

Stand-alone Server Cover Replacement (If Not Racked)

Insert the Server from the Front (If Racked)

HotSwap Chassis Fan

Front Bezel Removal (Single Piece)

Front Bezel Removal (Two Piece)

HotSwap Chassis Fan Cover Removal

HotSwap Chassis Fan Removal

HotSwap Chassis Fan Replacement

HotSwap Chassis Fan Cover Replacement

Front Bezel Replacement (Single Piece)

Front Bezel Replacement (Two Piece)

E C T
4.708
J
L - AC

Disk Drive

Front Bezel Removal (Single Piece)
Front Bezel Removal (Two Piece)
HotPlug Disk Drive Removal
HotPlug Disk Drive Replacement
Front Bezel Replacement (Single Piece)
Front Bezel Replacement (Two Piece)

Display Board

Front Bezel Removal (Single Piece)
Front Bezel Removal (Two Piece)
HotSwap Chassis Fan Cover Removal
HotSwap Chassis Fan Removal
Display Board Removal
Display Board Replacement
HotSwap Chassis Fan Replacement
HotSwap Chassis Fan Cover Replacement
Front Bezel Replacement (Single Piece)
Front Bezel Replacement (Two Piece)

Front Bezel

Front Bezel Removal (Single Piece)
Front Bezel Removal (Two Piece)
Front Bezel Replacement (Single Piece)
Front Bezel Replacement (Two Piece)
One Piece Bezel Install

Memory DIMM

Extend the Server out the Front (If Racked)
Stand-alone Server Cover Removal (If Not Racked)
Top Cover Removal
Memory DIMM Removal
Memory DIMM Replacement
Top Cover Replacement
Stand-alone Server Cover Removal (If Not Racked)
Insert the Server from the Front (If Racked)

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1079
Doc:

PCI I/O Card

Extend the Server out the Front (If Racked)
Stand-alone Server Cover Removal (If Not Racked)
Side Cover Removal
PCI I/O Card Removal
PCI Card Separator/Extractor Removal
PCI Card Separator/Extractor Replacement
PCI I/O Card Replacement
Side Cover Replacement
Stand-alone Server Cover Replacement (If Not Racked)
Insert the Server from the Front (If Racked)

Power Supply

Front Bezel Removal (Single Piece)
Front Bezel Removal (Two Piece)
HotSwap Power Supply Removal
HotSwap Power Supply Replacement
Front Bezel Replacement (Single Piece)
Front Bezel Replacement (Two Piece)

HotSwap Power Converter Fan

HotSwap Power Converter Fan Removal
HotSwap Power Converter Fan Replacement

Platform Monitor

Extend the Server out the Front (If Racked)
Stand-alone Server Cover Removal (If Not Racked)
Top Cover Removal
Platform Monitor Removal
Platform Monitor Replacement
Top Cover Replacement
Stand-alone Server Cover Replacement (If Not Racked)
Insert the Server from the Front (If Racked)

E C T
4.706
J
L - AC

Processor Support Module

Extend the Server out the Front (If Racked)

Stand-alone Server Cover Removal (If Not Racked)

Top Cover Removal

Processor Support Module Removal

Processor Support Module Replacement

Top Cover Replacement

Stand-alone Server Cover Removal (If Not Racked)

Insert the Server from the Front (If Racked)

ROS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1620
Doc: 3707

Individual Component Remove/Replace Instructions

Each component has instructions for removal followed by instructions for replacement.

Extend the Server out the Front

rp54xx servers are available in two housings: rack-mounted or stand-alone. Access to servers mounted in an HP-supported rack is covered in this section.

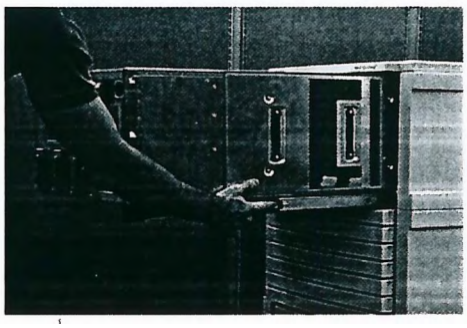
NOTE Ensure that there is enough area (Approximately 1.5 meters (4.5 ft) to fully extend the server out the front and work on it.

WARNING **Ensure that all anti-tip features (front and rear anti-tip feet installed; adequate ballast properly placed, etc.) are employed prior to extending the server.**

To extend the server, perform the following steps:

1. Remove the four T-25 screws that fasten the server to the rack.
2. Grasp the server chassis and slowly pull forward. The server is fully extended when the rail clips are locked in place. When fully extended, the top and side service bays are fully accessible.

The following graphic shows the server extended and indicates the rail clip location.



E C T
4.704
I
J
L A C

Insert the Server from the Front

rp54xx servers are available in two housings: rack-mounted or stand-alone. Access to servers mounted in an HP-supported rack is covered in this section.

To return the server into the rack, press the rail clips on either side of the server in and push the server into the rack until it stops.

The following graphic shows the server extended and indicates the rail clip location.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1621
Fls: 127
3701
Doc:

Stand-alone Server Cover Removal

The rp54xx server can be ordered as a stand-alone unit. In this configuration, the server has a one-piece protective cover over it and sits on a platform with locking wheels attached.

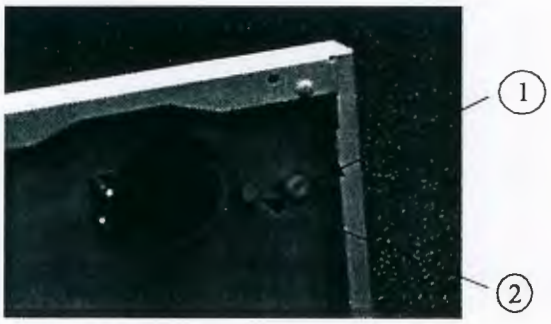
To remove the cover from a stand-alone server, perform the following procedures:

1. Unfasten and remove the screws (with captive washers) located near the bottom edge of both sides of the server cover.
2. Lift the protective cover off of the server and set it aside.

WARNING **The stand-alone server weights 69 kg (150 lbs). Removing the stand-alone server from its platform requires three people or a suitable lifting device. Failure to heed this precaution can result in serious personal injury or destruction of the server.**

To remove the server from its wheeled platform, perform the following procedure:

1. Facing the front of the server, reach under the platform on the right side and unfasten the knurl-knobbed, spring-loaded pin (item 1). The pin will retract when it is free. Perform the same step at the rear of the server. The rear knurl-knobbed, spring-loaded pin is aligned behind the front pin, but at the rear of the server.

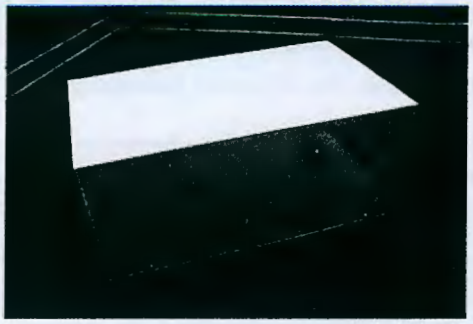


2. From the back of the server, reach under the platform, behind the knurl-knobbed, spring-loaded pin, and locate the flat head of the second spring-loaded pin (item 2). This pin is spring-loaded to stay up and keep the server from sliding on the platform. Pull the pin down and twist one quarter turn to the left to lock the pin down and out of the way. Perform the same step at the front of the server.
3. The server is now free from its wheeled platform and can be removed from it.

WARNING **The stand-alone server weights 69 kg (150 lbs). Removing the stand-alone server from its platform requires three people or a suitable lifting device. Failure to heed this precaution can result in serious personal injury or destruction of the server.**

E C T
4.702
J
CPL - AC

The following graphic shows the protective cover.



RQS Nº 03/2005 - CN
CPMI - CORREIOS
1622
Fls:
3701
Doc:

Stand-alone Server Cover Replacement

The rp54xx server can be ordered as a stand-alone unit. In this configuration, the server has a one-piece protective cover over it and sits on a platform with locking wheels attached.

To place the server on its wheeled platform, perform the following procedure:

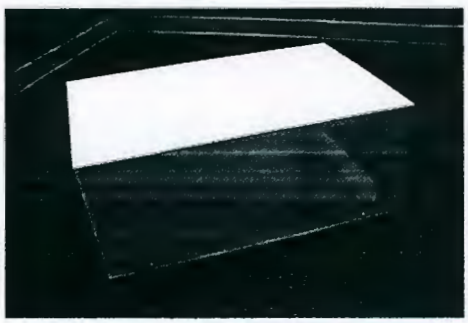
WARNING **The stand-alone server weights 69 kg (150 lbs). Placing the stand-alone server on its platform requires three people or a suitable lifting device. Failure to heed this precaution can result in serious personal injury or destruction of the server.**

1. Lift the platform and turn both of the spring-loaded, flat-headed pins (item 1) a quarter turn to the right to lock them out of the way before placing the server on the platform.
2. Using a lifting devise or a minimum of three people, lift the server onto the platform. Align the server and platform so that the pins will lock.
3. Reach under the platform, locate the spring-loaded, flat headed pins and turn them one quarter turn to the left to unlock them. Gently slide the server around on the platform until the spring-loaded flat-head pins snap into their holes.
4. Once again, reach under the platform on the right side and fasten both front and back knurl-knobbed, spring-loaded pins (item 2).

To place the cover on a stand-alone server, perform the following procedures:

1. Set the protective cover on the server and align the holes located near the bottom edge of both sides of the server cover.
2. Fasten the screws (with captive washers) through the cover, into the platform.

The following graphic shows the protective cover.



E C T
4.700
L - AC

Top Cover Removal

The power to the server does not have to be off to remove the top cover and air baffle. However, operation of the server without the top cover in place can make it susceptible to EMI problems.

Follow the steps listed below to remove the top cover:

1. Loosen the captive T-15 screws that hold the top cover in place.
2. Grasp the strap handles, raise the cover slightly, and pull the cover toward the front of the server to free the cover tabs from the slots in the chassis. The air baffle will be exposed.

Loosen the captive T-15 screws that hold the air baffle in place then lift the air baffle off of the server.

The following graphics show the top service bay cover and the air baffle. The first graphic shows the top service bay cover.

The second shows the air baffle.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1623
Doc: 3701

Top Cover Replacement

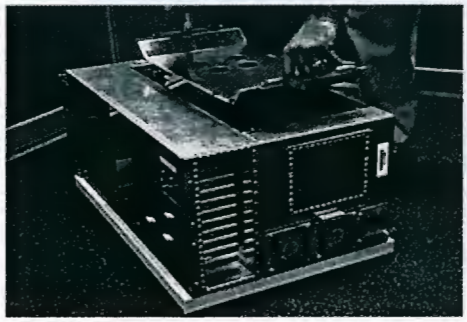
The power to the server does not have to be off to remove or replace the top service bay cover and air baffle. However, operation of the server without the top cover in place can make it susceptible to EMI problems.

Set the air baffle in place over the opening for the top service bay and tighten the captive T-15 screws.

Follow the steps listed below to replace the top cover:

1. Align the tabs on the end of the top cover with the corresponding slots in the chassis and seat the tabs fully into the slots.
2. Seat the top cover in the top of the service bay and tighten the captive T-15 screws that hold the cover in place.

The following graphics show the air baffle and the top service bay cover. The first graphic shows the air baffle.



The second graphic shows the top service bay cover.

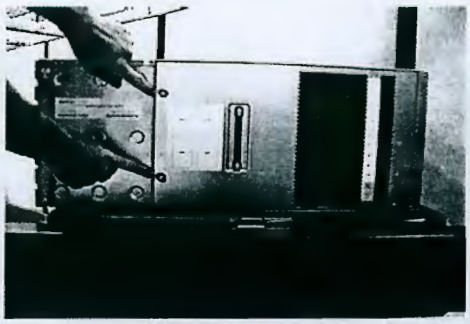
ECT 4.698 I 9 AC

Side Cover Removal

The Side Cover protects the side service bay. The power to the server does not have to be off to remove the side cover. However, operation of the server without the side cover in place can make it susceptible to EMI problems.

Loosen the captive T-15 screws that hold the side cover in place, then grasp the strap handle and pull the cover away from the server.

The following graphic shows the side cover with captive screw locations.



RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1624
Doc: 3701

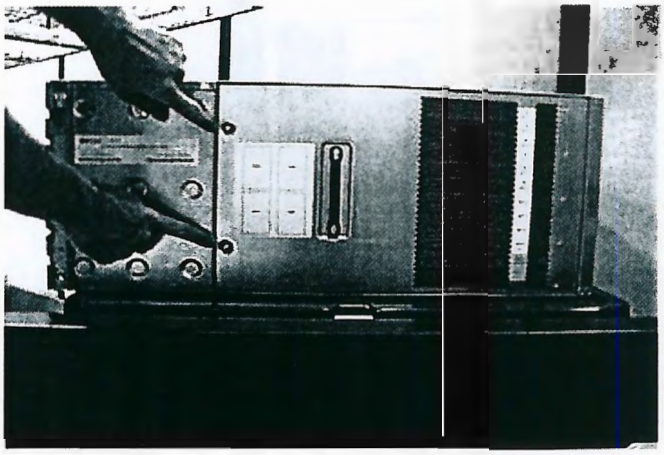
Side Cover Replacement

The power to the server does not have to be off to replace the side cover. However, operation of the server without the side cover in place can make it susceptible to EMI problems.

Replace the side cover according to the following steps:

1. Grasp the strap handle and insert the tabbed end of the cover into the server chassis slots on the right side of the side service bay.
2. Push the cover into the side service bay opening and fasten the captive T-15 screws that hold the side cover in place.

The following graphic shows the side cover with captive screw locations.



FLS
14.696
3
AC

Front Bezel Removal (Single Piece)

The rp54xx server front bezel is hinged on the left (facing the front of the server). The server does not have to be turned off to open or to completely remove the bezel.

Opening the door provides access to the following components:

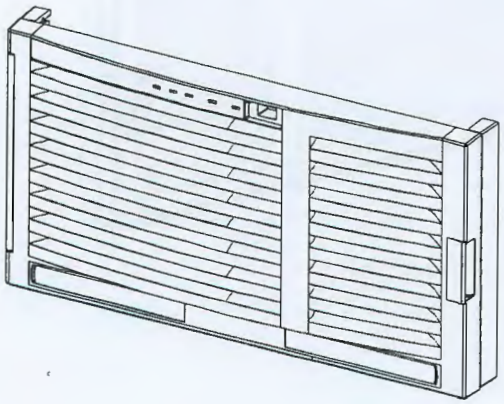
- HotPlug Disks (A0, A1, and B0, B1).
- Removable Media (CD-ROM drive, etc.).
- HotSwap Chassis Fan cover.
- HotSwap Chassis Fan 0.
- HotSwap Power Supplies (up to three).

To open the front bezel, grasp the right edge of the bezel and pull out. The bezel will swing away from the chassis.

To remove the entire bezel, perform the following steps:

1. Open the front bezel and swing it to the left as far as possible.
2. Pry the hinge cover, located on the left side of the server, off the chassis.
3. While supporting the bezel, remove the screws that secure the bezel hinge to the left side of the server.
4. Grasp the left side of the bezel and pull it loose.

The following graphic shows the front bezel.



RQS Nº 03/2005 - CN
CPMI - CORREIOS
1625
Fls:
3701
Doc:

Front Bezel Replacement (Single Piece)

The rp54xx server front bezel is hinged on the left (facing the front of the server). The server does not have to be turned off to open or to completely remove the bezel.

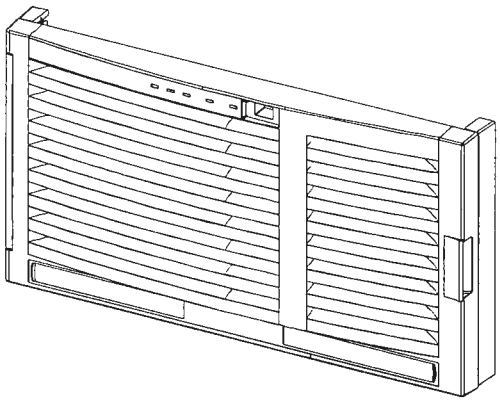
The bezel encloses the following components:

- HotPlug Disks (A0, A1, and B0, B1).
- Removable Media (CD-ROM drive, etc.).
- HotSwap Chassis Fan cover.
- HotSwap Chassis Fan 0.
- HotSwap Power Supplies (up to three).

To attach the bezel, perform the following steps:

1. Screw the bezel hinge to the threaded inserts on the left side of the server.
2. Install the hinge cover by aligning the notch in the top of the cover with the top of the assembly cover and press firmly into place.

   The following graphic shows the front bezel.



Front Bezel Removal (Two Piece)

The rp54xx server front bezel is divided and hinged on the right (facing the front of the server) side to provide a door for Disk Media Bay access. The server does not have to be turned off to open the access door or to completely remove the bezel.

Opening the door provides access to the following components:

- HotPlug Disks (A0, A1, and B0, B1).
- Removable Media (CD-ROM drive, etc.).

Removing the entire bezel provides access to the components listed above and the following:

- HotSwap Chassis Fan cover.
- HotSwap Chassis Fan 0.
- HotSwap Power Supplies (up to three).

To open the Disk Media access door, grasp the right edge of the door and pull out. The door will swing away from the chassis, exposing the Disk Media Bay.

To remove the entire bezel, perform the following steps:

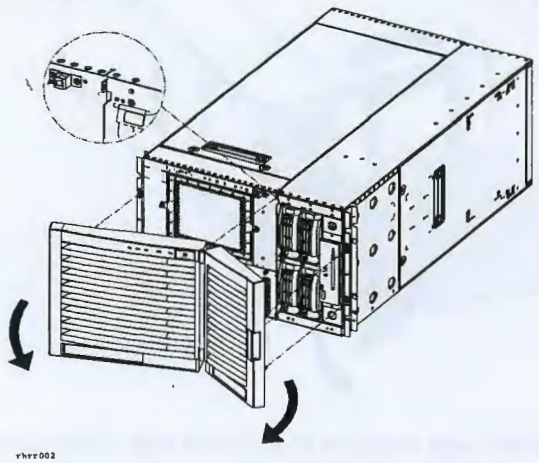
1. Open the Disk Media access door, exposing the plastic bezel pins inserted in the clips at the top and bottom of the Disk Media bay on the left side.
2. Grasp the left side of the bezel and pull it loose.

CAUTION DO NOT try to pull the bezel off of the server at this point. The plastic pins holding the bezel on the right side are inserted in metal clips on the Disk Media bay and if the plastic pins are bent, they will break off.

---

3. Grasp the bezel with both hands and carefully slide the bezel to the left until both plastic pins clear the metal clips on the Disk Media bay.
4. Pull the bezel away from the server and set it aside.

The following graphic shows the front bezel.



RQS Nº 03/2005 - CN
CPMI - CORREIOS
1626
Fls:
Doc: 3701

Front Bezel Replacement (Two Piece)

The rp54x0 server front bezel is divided and hinged on the right (facing the front of the server) side to provide a door for Disk Media Bay access. The server does not have to be turned off to open the access door or to completely remove the bezel.

The Disk Media Bay door encloses the following components:

- HotPlug Disks (A0, A1, and B0, B1).
- Removable Media (CD-ROM drive, etc.).

The left side of the front bezel encloses the following components:

- HotSwap Chassis Fan cover.
- HotSwap Chassis Fan 0.
- HotSwap Power Supplies (up to three).

To attach the bezel, perform the following steps:

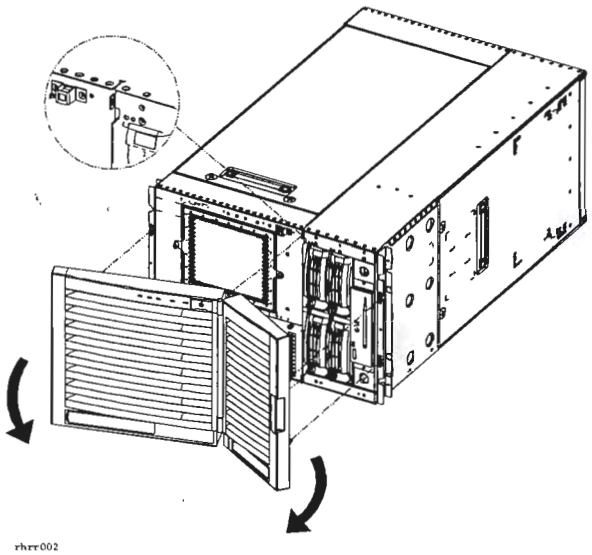
1. Swing the Disk Media access door open so that the plastic pins that go into the metal clips on the Disk Media bay are exposed.

CAUTION The plastic pins holding the bezel on the right side are inserted into metal clips on the Disk Media bay. DO NOT bend the plastic pins or they will break off.

---

2. Holding the bezel with both hands, align the bezel pins with the metal clips on the Disk Media bay and carefully slide the bezel pins into the clips.
3. Attach the left side of the bezel to the server chassis by aligning the bezel pins with the chassis clipsand press the bezel into the chassis until the pins snap into the clips.

   The following graphic shows the front bezel.



rhrr002

4. Swing the Disk Media access door closed and attach it to the right side of the server chassis.

ECT 4.6921 V AC

Core I/O Removal

rp54xx Core I/O functions are contained on the GSP revision A/B and LAN/SCSI cards. Both cards are located on the PCI Backplane in the side service bay. The LAN/SCSI card is in I/O slot 1 and the GSP revision A/B card is in I/O slot 2.

Before removing either of the Core I/O cards from the server, perform the following tasks:

- Power down the server.
- Detach all power cords from the server.

To remove a Core I/O card from the server, perform the following steps:

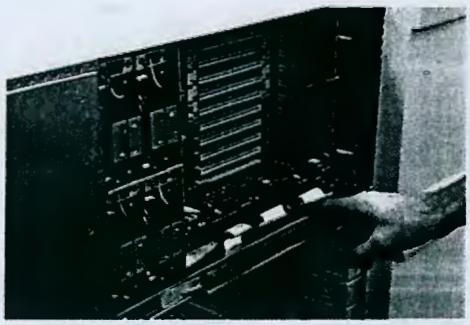
1. Remove all cables attached to the Core I/O card at the rear bulkhead.

NOTE Be sure to label the cables before removing them.

---

2. Disconnect any ribbon cable connectors attached to the Core I/O card in the side service bay.
3. Grasp the edge of the Core I/O card and pull it out of the server.

The following graphic shows both Core I/O cards in the side service bay.



RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1627
Doc: 3701

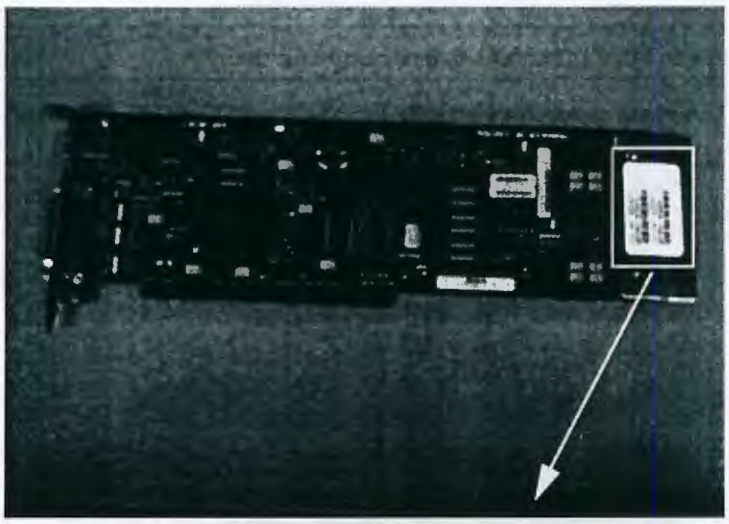
Core I/O Replacement

rp54xx Core I/O functions are contained on the GSP and LAN/SCSI cards. Both cards are located on the PCI Backplane in the side service bay. The LAN/SCSI card is in I/O slot 1 and the GSP card is in slot 2.

Before replacing either of the Core I/O cards, perform the following tasks:

- Power down the server.
- Detach all power cords from the server.

NOTE For revision B GSP only, remove *one* of the MAC address labels and place on the rear of the server as shown in the following graphics.



To replace a Core I/O card, perform the following steps:

ECT 1
24.690
J
CPL - AC

1. Orient the I/O card in its guide and push it into the server until the card connector seats in the I/O Backplane card slot.
2. Connect the I/O cable attached to the I/O card at the rear PCI bulkhead.
3. Connect any ribbon cable connectors attached to the I/O card in the side service bay.

The following graphic shows an I/O card being replaced.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1628
Fls:
Doc: 3701

PCI Card Separator/Extractor Removal

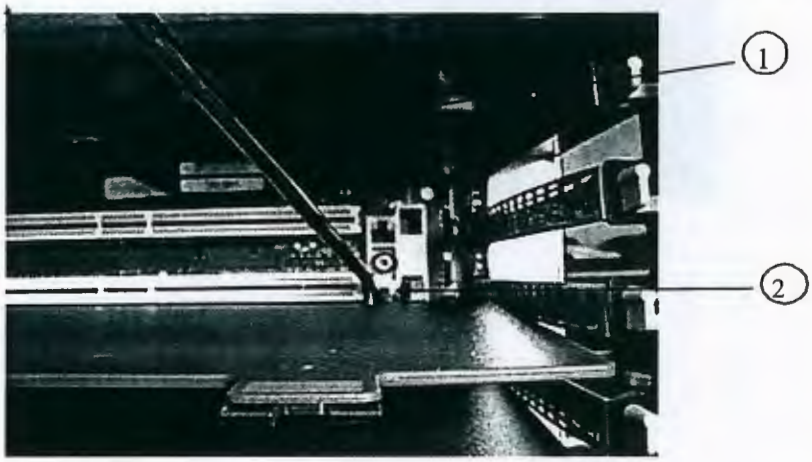
PCI card separator/extractors are located in the Side Service Bay, between the PCI cards. PCI card separator/extractors are plastic cards with two tab handles and two LEDs.

Before removing a PCI card separator/extractor from the server, perform the following tasks:

- Shut down the server.
- Remove the corresponding PCI card.

To remove a PCI card separator/extractor, perform the following steps:

1. Carefully slide a long shaft, medium width, flat blade screw driver (item 1) into the Side Service Bay along the side of the PCI card separator/extractor, and insert it into the slot in the hook tab (item 2).



2. At the point where the PCI card separator/extractor inserts into the PCI backplane connector (item 2), there are two slotted, hook tab connectors on the PCI card separator/extractor, one on either side of the PCI Backplane connector. Press one then the other to disengage the card from the backplane.
3. With the two connection points pressed, slide the PCI card separator/extractor out of the PCI card cage.

PCI Card Separator/Extractor Replacement

PCI card separator/extractors are located in the Side Service Bay on the PCI Backplane, between PCI cards. PCI card separator/extractors are plastic cards with two tab handles and two LEDs.

To replace a PCI card separator/extractor, perform the following steps:

1. Insert the PCI card separator/extractor into the available slot and slide it into the PCI backplane connector.
2. Be sure the two hook tabs on the PCI card separator/extractor insert into the connector blocks on either side of the PCI backplane.

Once you have completed replacement of the PCI card separator/extractor into the server, perform the following tasks:

- Replace the PCI card, if necessary.
- Power up the server.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1629
Fls:
Doc:

HotPlug Disk Drive Removal

The internal disk drives (up to four) are located at the front right side of the server (as you are facing it). When proper software and hardware procedures are followed, internal disk drives can be removed and replaced while the server is running.

The procedures in this section are in two parts, a HotSwap Software Procedure and a HotPlug Hardware Procedure, for removing the disk from the server.

Before starting these procedures, you must have an up-to-date configuration backup file. Configuration backup is performed by default each time an LVM command changes the LVM configuration. The default backup files path is:

`/etc/lvmconf/base_vg_name.conf.`

The replacement disk drive must be the same product ID as the disk drive that is being replaced.

NOTE HP often uses different manufacturers for disks that have the same product number. The HotSwap and HotPlug procedures will not update the disk drive's internal information to that of the replaced disk drive.

The replacement disk drive will have the same capacity and blocksize as the defective disk because they have the same product number. The only field that can be incorrect is the string specifying the vendor's name. This will not affect the behavior of the LVM. If you desire to update the manufacturer's name, the disks volume group must be deactivated and reactivated.

HotSwap Software Procedure

Perform these software procedural steps to replace a HotPlug disk drive device:

Step 1. Determine whether LVM found the physical volume to be defective when the volume group was activated.

If the volume was defective when the volume group was activated, *vgchange* will generate the following message to the console:

```
WARNING

VGCHANGE: WARNING: COULDN'T ATTACH TO THE VOLUME GROUP PHYSICAL
VOLUME "/DEV/DSK/cXtXdX"

VGCHANGE: WARNING: COULDN'T ATTACH TO THE VOLUME GROUP PHYSICAL
VOLUME "/DEV/DSK/cXtXdX"

THE PATH OF THE PHYSICAL VOLUME REFERS TO A DEVICE THAT DOES NOT
EXIST, OR IS NOT CONFIGURED INTO THE KERNAL.
```

If you are unsure of the status of *vgchange*, check it with the *vgdisplay* command:

#vgdisplay <VG name>

For example:

vgdisplay /dev/vg00

If the disk was defective when the *vgchange* command was entered, the following message will be printed one or more times:

E C T
4.686
1
V
A C

```
WARNING:

VGDISPLAY: WARNING: COULDN'T QUERY PHYSICAL VOLUME "/DEV/DSK/cXtXdX"
THE SPECIFIED PATH DOES NOT CORRESPOND TO PHYSICAL VOLUME ATTACHED TO THE
VOLUME GROUP.

VGDISPLAY: WARNING: COULDN'T QUERY ALL OF THE PHYSICAL VOLUMES.
```

If you see these messages, the disk was defective at the time the volume group was activated. Remove the bad disk as described in step 9 of this procedure, then follow the instructions in for replacing the disk and perform the *HotSwap Procedure for Unattached Physical Volumes* described there.

Otherwise, the disk drive became defective after *vgchange* was run. Proceed to Step 2.

Step 2. Display the names of all the logical volumes on this volume group with the *vgdisplay* command. For example:

```
#vgdisplay /dev/vg00
```

Step 3. Determine which logical volumes have mirrors with the *lvdisplay* command. For example:

```
#lvdisplay /dev/vg00/lvol# | grep -ie "LV Name" -e "Mirror"
```

Step 4. Determine the *pvkey* command status for the mirrored logical volume, again using the *lvdisplay* command with the *-k* option. Compare the output to the *lvdisplay* command with the *-v* option to determine the device file to *pvkey* mapping. For example,

```
# lvdisplay -v -k /dev/vg00/lvol1
--- Logical volumes ---
LV Name                     /dev/vg00/lvol1
VG Name                     /dev/vg00
LV Permission               read/write
LV Status                   available/syncd
Mirror copies               1
Consistency Recovery        MWC
Schedule                    parallel
LV Size (Mbytes)            256
Current LE                  64
Allocated PE                128
Stripes                     0
Stripe Size (Kbytes)        0
Bad block                   off
Allocation                  strict/contiguous
IO Timeout (Seconds)        default

   --- Distribution of logical volume ---
   PV Name            LE on PV  PE on PV
   /dev/dsk/c1t6d0    64        64
   /dev/dsk/c2t6d0    64        64

   --- Logical extents ---
   LE    PV1                 PE1   Status 1 PV2                 PE2   Status 2
   00000      0              00000 current       1              00000 current
   00001      0              00001 current       1              00001 current
   00002      0              00002 current       1              00002 current
```

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1630
Fls:
3701
Doc:

```
   00003       0             00003 current       1             00003 current
   00004       0             00004 current       1             00004 current
   00005       0             00005 current       1             00005 current
   00006       0             00006 current       1             00006 current
   00007       0             00007 current       1             00007 current
   00008       0             00008 current       1             00008 current
(etc.)
```

```
# lvdisplay -v /dev/vg00/lvol1
--- Logical volumes ---
LV Name                     /dev/vg00/lvol1
VG Name                     /dev/vg00
LV Permission               read/write
LV Status                   available/syncd
Mirror copies               1
Consistency Recovery        MWC
Schedule                    parallel
LV Size (Mbytes)            256
Current LE                  64
Allocated PE                128
Stripes                     0
Stripe Size (Kbytes)        0
Bad block                   off
Allocation                  strict/contiguous
IO Timeout (Seconds)        default

   --- Distribution of logical volume ---
   PV Name            LE on PV  PE on PV
   /dev/dsk/c1t6d0    64        64
   /dev/dsk/c2t6d0    64        64

   --- Logical extents ---
   LE    PV1                 PE1   Status 1 PV2                 PE2   Status 2
   00000 /dev/dsk/c1t6d0     00000 current  /dev/dsk/c2t6d0     00000 current
   00001 /dev/dsk/c1t6d0     00001 current  /dev/dsk/c2t6d0     00001 current
   00002 /dev/dsk/c1t6d0     00002 current  /dev/dsk/c2t6d0     00002 current
   00003 /dev/dsk/c1t6d0     00003 current  /dev/dsk/c2t6d0     00003 current
   00004 /dev/dsk/c1t6d0     00004 current  /dev/dsk/c2t6d0     00004 current
   00005 /dev/dsk/c1t6d0     00005 current  /dev/dsk/c2t6d0     00005 current
   00006 /dev/dsk/c1t6d0     00006 current  /dev/dsk/c2t6d0     00006 current
   00007 /dev/dsk/c1t6d0     00007 current  /dev/dsk/c2t6d0     00007 current
   00008 /dev/dsk/c1t6d0     00008 current  /dev/dsk/c2t6d0     00008 current
```

The *pvkey* stuatus (0 or 1 in this example) shown in the first command, maps to the device file names (*/dev/dsk/c1t6d0* or */dev/dsk/c2t6d0*) in the second command under columns *PV1* and *PV2*, respectively.

Step 5. Reduce any logical volumes that have mirror copies on the faulty disk drive so that they no longer mirror onto that disk drive (note the *-A n* option):

```
# lvreduce -m 0 -A n -k <LV name> /dev/dsk/cXtXcX <pvkey#>&
```

ECT 14.684 CPL - AC

(for 1 way mirroring)

OR

```
# lvreduce -m 1 -A n -k <LV name> /dev/dsk/cXtXcX <pvkey#>&
```

(for 2way mirroring)

For example, enter:

```
# lvreduce -m 0 -A n -k /dev/vg00/lvol4 /dev/dsk/c2t4d0 1&
```

The following message will appear:

```
Logical volume /dev/vg00/lvol4 has been successfully reduced.
lvlnboot: Logical Volume has no extents.
```

NOTE It is important to include the ampersand (&) at the end of the command line. Otherwise, the *lvreduce* process will hang, and you will need terminal control to negate the command. Once the 'successfully reduced' message has been generated, manually end the process using the *kill -9* command.

Step 1. Use the *ps* command to find the PID for the *lvreduce* process.

```
# ps -ef | grep lvreduce
```

Step 2. Manually end the process with the *Kill -9* command (It may take several minutes for the process to end.).

```
# kill -9 <PID>
```

Step 3. Repeat steps 4 and 5 for all logical volumes.

Step 4. With all logical volumes reduced, now reduce the volume group using the *vgreduce* command. For example:

```
# vgreduce /dev/vg00 /dev/dsk/c2t6d0
```

CAUTION The *vgreduce* procedure may take a long time to complete. Do NOT terminate this process.

Step 5. Update the disk BDRA using the `lvlnboot` command.

```
# lvlnboot -R
```

Step 6. Proceed to the *HotPlug Hardware Procedure* to remove the bad disk drive from the server.

HotPlug Hardware Procedure

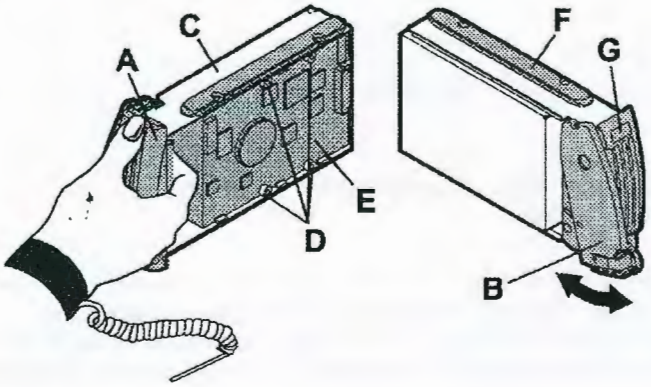
CAUTION Disk Drives can be removed or installed with the server still powered on. This is referred to as a "manual HotPlug".

To remove a disk drive from the server, perform the following step:

ROS Nº 03/2005 - CN
CPMI - CORREIOS
1631
Fls: 3701
Doc:

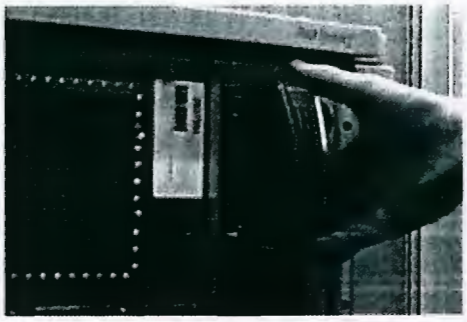
Grasp the tab at the bottom of the cam latch on the selected disk drive, then push the button inside the cam latch and pull the cam latch out and up. The disk drive will unlock. Pull gently until it slides completely free.

The following graphic shows disk features.



A bezel handle
B cam latch
C carrier frame
D standoffs
E circuit board
F insertion guide
G capacity label

The next graphic depicts disk removal/replacement.



HotPlug Disk Drive Replacement

The internal disk drives (up to four) are located at the front right side of the server (as you are facing it). When proper software and hardware procedures are followed, internal disk drives can be removed and replaced while the server is running.

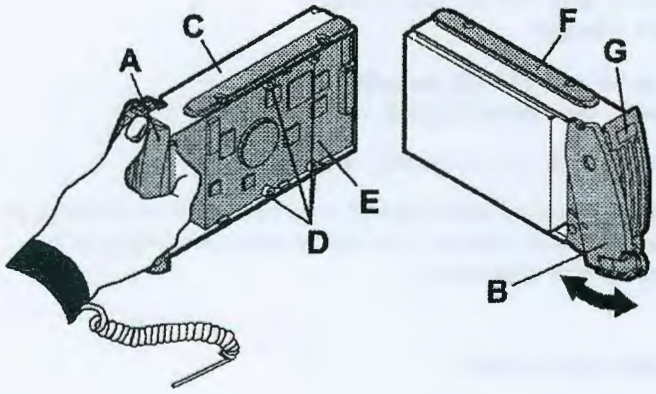
CAUTION Disk Drives can be removed or installed with the server still powered on. This is referred to as a "manual HotPlug".

However, DO NOT replace a HotPlug disk drive until a controlled shutdown of the operating system has been performed.

Hardware HotPlug Procedure

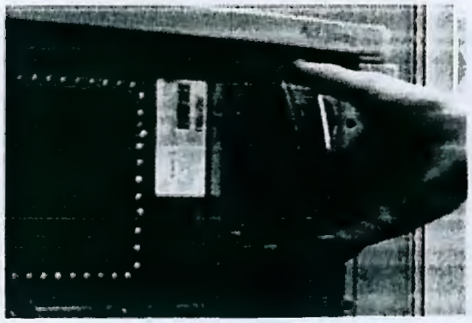
To replace a disk drive in the server, grasp the tab at the bottom of the cam latch on the selected disk drive, push the button inside the cam latch, and pull the cam latch out and up. The disk drive will unlock. Pull gently until it slides completely free.

The following graphic shows disk features.

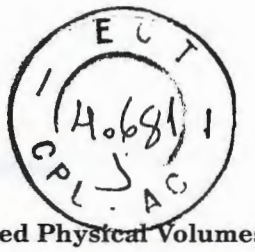


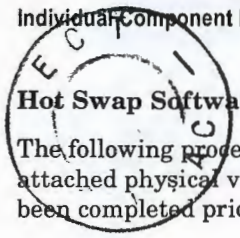
- **A** bezel handle
- **B** cam latch
- **C** carrier frame
- **D** standoffs
- **E** circuit board
- **F** insertion guide
- **G** capacity label

The next graphic depicts disk removal/replacement.



RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1632
3701
Doc:





Hot Swap Software Procedure for Attached Physical Volumes

The following procedure is an example of how to recover from replacing a disk that was recognized as an attached physical volume. Be sure that all the software procedures in the *Disk Drive Removal* section have been completed prior to starting these steps. This example assumes that the disk was mirrored.

NOTE HP often uses different manufacturers for disks, but assigns the same product number. The hot swap manual procedure will not update disk driver internal information to that of the replaced disk drive.

Step 1. Perform an *ioscan* on the replaced disk drive to ensure that it is accessible (claimed), to double check that it is a proper replacement, and that the device files are present. Refer to the above note.

For example: `# ioscan -fnC disk`

Step 2. Use the following procedure to mirror the root disk:

a. Create the new physical volume using the *pvcreate* command.
For example: `# pvcreate -B /dev/rdsk/cXtXdX`

b. Extend the volume group to include the new physical volume using the *vgextend* command:
For example: `# vgextend /dev/vg00 /dev/dsk/cXtXdX`

c. The *mkboot* command must be run to make the device bootable.
For example:`# mkboot /dev/rdsk/cXtXdX`

d. Use the *mkboot* command again to add the HP-UX auto-file-string.
For example: `# mkboot -a "hpux" /dev/rdsk/cXtXdX`

e. Run *lvlnboot* with the following command: `# lvlnboot -R`

f. Run *lvextend* to put a mirror into the replaced disk drive. It may take several minutes to copy the original copy of the data to the mirrored extents. The logical volume(s) will still be accessible to user applications during this operation.

For example:
```
# lvextend -m 1 <LV name> /dev/dsk/cXtXdX
```
OR
```
# lvextend -m 2 <LV name> /dev/dsk/cXtXdX (for 3 way mirroring)
```

For example:
```
# lvextend -m 1 /dev/vg00/lvol4 /dev/dsk/cXtXdX
```
OR
```
# lvextend -m 1 /dev/vg00/lvol5 /dev/dsk/cXtXdX
```

Repeat this for each logical volume to be mirrored.

Verify that the mirror is bootable and AUTO file is correct.

```
For example:
# lifls -l /dev/rdsk/cXtXdX
```
OR
```
# lifcp /dev/rdsk/cXtXdX:AUTO -
```

ECT 4.680 CPL - AC

g. Verify that the mirroring is set up properly.

For example:

```
# vgdisplay -v /dev/vg00
# lvdisplay /dev/vg00/lol1 - lvol8
# lvlnboot -v /dev/vg00
```

Both disks should list as "Boot Disk" and both should appear in the *lvol* lists.

At this point the system will be fully functional.

Hot Swap Procedure for Unattached Physical Volumes

The following steps are an example of how to replace a HotPlug disk drive for unattached physical volumes. This example assumes the disks are mirrored.

NOTE HP often uses different manufacturers for disks, but assigns the same product number. The hot swap manual procedure will not update disk driver internal information to that of the replaced disk drive.

Step 1. Perform an *ioscan* on the replaced disk drive to ensure that it is accessible (claimed), to double check that it is a proper replacement, and that the device files are present. Refer to the above note.

For example: `# ioscan -fnC disk`

Step 2. Restore the LVM configuration/headers onto the replaced disk drive from your backup of the LVM configuration with the following entry:

```
# vgcfgrestore -n <volume group name> /dev/rdsk/cXtXdX
```

For example: `# vgcfgrestore -n /dev/vg00 /dev/rdsk/cXtXdX`

Step 3. Attach the new disk drive to the active volume group with the following *vgchange* command:

```
# vgchange -A y <volume group name>
```

For example: `# vgchange -A y /dev/vg00`

Step 4. Use the *mkboot* command to make the device bootable.

For example: `# mkboot /dev/rdsk/cXtXdX`

Step 5. Use the *mkboot* command again to add the HP-UX auto-file-string.For example: `# mkboot -a "hpux" /dev/rdsk/cXtXdX`

Step 6. Run *lvlnboot* with the following command: `# lvlnboot -R`

Step 7. Resynchronize the mirrors of the replaced disk drive with the following command. It may take several minutes to copy all the data from the original copy of the data to the mirrored extents. The logical volume(s) are still accessible to users' applications during this command.

```
# vgsync <VG name>
```

For example: `# vgsync /dev/vg00`

At this point the system will be fully functional.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1633
Fls:
Doc: 3701

HotSwap Chassis Fan Cover Removal

Power to the server does not have to be off to remove or replace a HotSwap Chassis fan cover. Fan number 0 is in the front of the server and fan number 1 is at the rear of the server.

To remove a fan cover from the server, perform the following steps:

1. Loosen the captive T-15 screws from the sides of the cover.
2. Gently pry the cover away from the server and set it aside.

The following graphic shows a Chassis Fan Cover in place.

4.678 1
CPL - 3
AC

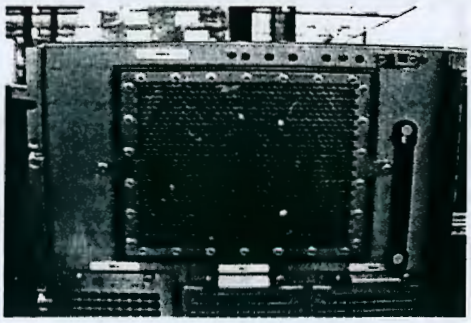
HotSwap Chassis Fan Cover Replacement

The power to the server does not have to be off to remove or replace a HotSwap Chassis Fan cover. Fan number 0 is located in the front of the server and fan number 1 is located at the rear of the server.

To replace a chassis fan cover, perform the following tasks:

1. Insert the cover into position in front of the fan.
2. Tighten the captive T-15 screws on each side of the cover.

The following graphic shows a HotSwap Chassis Fan Cover.



RQS Nº 03/2005 - CN
CPMI - CORREIOS
1634
Fls:
Doc:

HotSwap Chassis Fan Removal

The power to the server does not have to be off to remove or replace a HotSwap Chassis fan. Fan number 0 is in the front of the server and fan number 1 is at the rear of the server.

To remove a fan from the server, perform the following steps:

1. Check the fan LED located on the fan. If the LED is illuminated, the fan has failed.

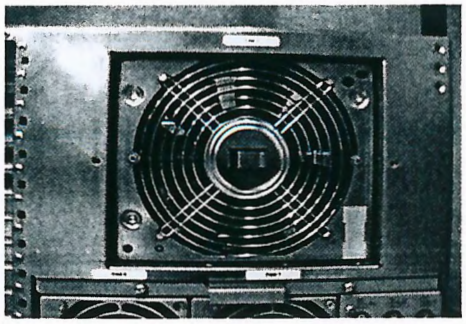
NOTE When one fan has failed (or is removed from the server), the system automatically puts the remaining fan into high speed mode. The noise level of the server will increase.

2. Grasp the fan grill and gently pull toward you. The fan assembly will unplug from the electrical outlet and slide out of the server.

CAUTION Running the server for extended periods of time with a cooling fan removed may create hot spots inside the server and possibly shorten component life.

If the other fan fails when one fan is removed, the system will halt.

The following graphic shows a HotSwap Chassis Fan.



4.762

HotSwap Power Supply Replacement

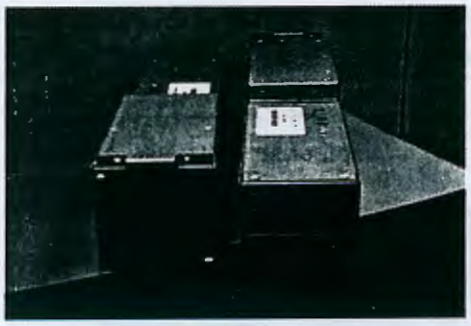
Up to three power supplies (0 through 2), located across the bottom front of the server, can be installed in the server without removing power.

To replace a power supply, perform the following steps:

CAUTION Be careful when putting the power supply into the server. It is heavier than it appears.

1. Grasp the handle in one hand and support the power supply with the other. Slide the power supply into the server. The Power Supply LED should illuminate immediately.
2. Replace the T-15 mounting screw located to the right of the handle near the top of the power supply.

The following graphic shows a front and rear view of a HotSwap Power Supply.



RQS Nº 03/2005 - CN
CPMI - CORREIOS
1635
Fls:
Doc:
3761

HotSwap Power Converter Fan Removal

The power to the server does not have to be off to remove or replace a HotSwap Power Converter fan. Fans numbered 6 and 7 are located in the rear of the server.

To remove a fan from the server, perform the following steps:

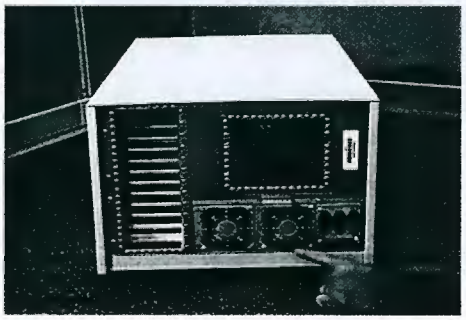
NOTE When one fan has failed (or is removed from the server), the system automatically puts the remaining fan into high speed mode. The noise level of the server will increase.

1. There are four screws attached to each corner of each fan. Loosen only the captive Torx-head screws located diagonally across the face of the fan (upper left, lower right sides).
2. Grasp the extended screw-heads (or the fan grill) and gently pull toward you. The fan assembly will unplug from the electrical outlet and slide out of the server.

CAUTION Running the server for extended periods of time with a cooling fan removed may create hot spots inside the server and possibly shorten component life.

If the other fan fails when one fan is removed, the system will halt.

The following graphic shows where HotSwap Power Converter Fans are located.



E C T
4.760
CPL - AC

HotSwap Power Converter Fan Replacement

The power to the server does not have to be off to remove or replace a HotSwap Power Converter fan. Fans numbered 6 and 7 are located in the rear of the server.

To replace a fan into the server, perform the following steps:

1. Orient the fan assembly so that the electrical plug will connect, then grasp the extended screw-heads (or the fan grill) and gently push the fan assembly into its housing. The fan assembly plug will connect with the electrical outlet in back of the housing.
2. Tighten the captive T-15 screws located diagonally across the face of the fan (upper left, lower right sides).

The following graphic shows where HotSwap Power Converter Fans are located.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1636
Fls:
Doc: 3791

Processor Support Module Removal

Processor Support Modules (PSMs) reside on the System Board and are accessed via the Top Service Bay. Looking into the Top Service Bay from the front, PSMs are located on either side of the server, at the front. There can be two PSMs, numbered 0 and 1

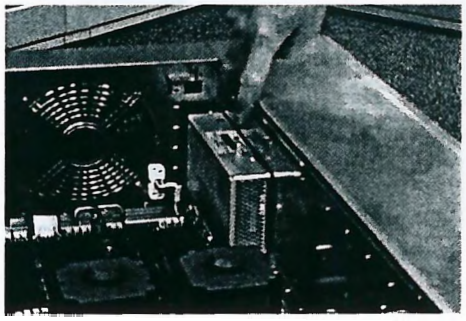
To remove a PSM from the server, perform the following steps:

1. Loosen the two captive mounting screws that hold the PSM in place.

NOTE For the rp5470, the mounting screws have been replaced by posts and the air baffle is used to secure the PSM's.

2. Grasp the two captive mounting screws and lift the PSM out of the server.

The following graphic shows a PSM in the server.



ECT 4.758 J CPL - AC

ECT CPL - AC

Processor Support Module Replacement

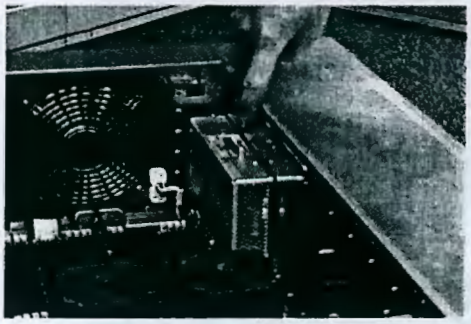
Processor Support Modules (PSMs) (there can be two PSMs, numbered 0 and 1) reside on the System Board and are accessed via the Top Service Bay. Looking into the Top Service Bay from the front, PSMs are located on either side of the server, at the front.

To replace a PSM, perform the following steps:

1. Seat the PSM into its socket.
2. Tighten the two captive mounting screws that hold the PSM in place.

NOTE For the rp5470, the mounting screws have been replaced by posts and the air baffle is used to secure the PSM's.

The following graphic shows a PSM in the server.



RQS Nº 03/2005 - CN
CPMI - CORREIOS
1637
Fls:
3701
Doc:

Memory DIMM Removal

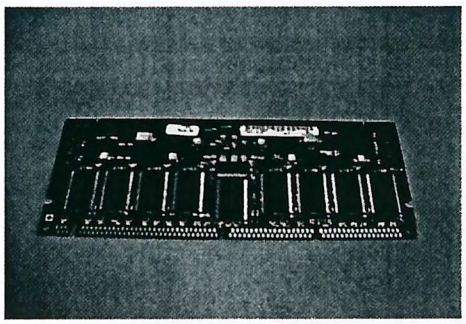
Memory DIMMs reside in slots (up to eight) located on the System Board. They are loaded in DIMM pairs of equal size.

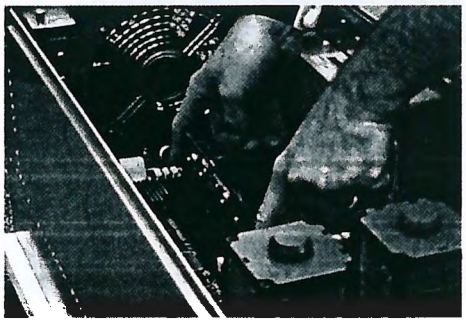
Removing rp5400 Memory DIMMs

To remove an rp5400 memory DIMM, perform the following steps:

1. Press down on the extractor levers on each end of the selected memory DIMM to unseat the DIMM from its socket.
2. When the memory DIMM unseats from the socket, pull it up and away from the System Board.

The following graphics show a memory DIMM, followed by a display of a DIMM being removed/replaced.





Removing rp5470 Memory DIMMs

To remove an rp5470 memory DIMM, perform the following steps:

1. Pull up on the extractor levers on each end of the Memory Carrier to unseat the Memory Carrier from its socket.
2. When the Memory Carrier unseats from the socket, pull it up and away from the System Board.
3. Loosen the captive screws that secure the DIMM Clip and remove DIMM Clip from the Memory Carrier.
4. Press down on the extractor levers on each end of the selected memory DIMM to unseat the DIMM from its socket.
5. When the memory DIMM unseats from the socket, pull it up and away from the Memory Carrier.

Memory DIMM Replacement

Memory DIMMs reside in slots located on the System Board (up to eight). They are loaded in DIMM pairs of equal size.

Replacing rp5400 and/or rp5450 Memory DIMMs

To replace a memory DIMM, perform the following steps:

1. Seat the memory DIMM into its socket.
2. Press the extractor levers on each end of the memory DIMM slot inward until the levers snap into place.

The following graphics show a memory DIMM and a display of DIMM removal/replacement.

Replacing rp5470 Memory DIMMs

To replace an rp5470 memory DIMM, perform the following steps:

1. Seat the memory DIMM into its socket on the Memory Carrier.
2. Press the extractor levers on each end of the memory DIMM slot inward until the levers snap into place.
3. Attach the Memory Clip to the Memory Carrier with the DIMM slot markings on the top of the Memory Clip aligned with the DIMM slot markings on the Memory Carrier. Secure the Memory Clip using the captive screws.
4. Seat the Memory Carrier into the slot on the System Board.
5. Push down on the extractor levers and snap them into place.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1638
Fls:
Doc: 3701

Display Board Removal

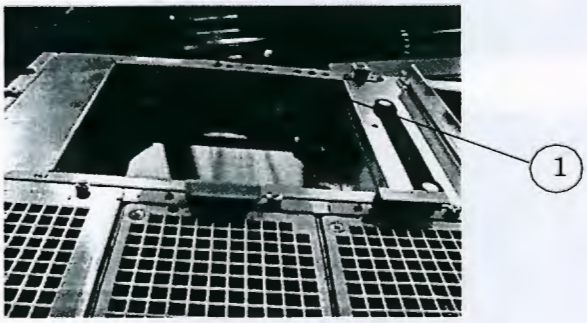
The Display Board contains the server's ON/OFF switch and five LEDs that indicate server status when power is applied.

CAUTION The Display Board is not a HotSwap or HotPlug unit. Ensure that the server is powered-down prior to removal.

To remove the Display Board, perform the following tasks:

1. Remove the three T-10 screws that hold the Display Board in place near the top of the chassis front.
2. Remove the two T-15 screws that hold the front Chassis Fan in place and extract the fan from the server.
3. Reach up through the top of the Chassis Fan cavity and carefully pull the Display Board back to free the LEDs and the On/Off switch from their chassis openings. Pull the Display Board down through the Chassis Fan cavity.
4. Disconnect the ribbon cable from the Display Board, and place the display board on a suitable work surface.

The following graphic shows the Display Board access location (item 1) (looking up from the bottom of the front of the server).



The next graphic shows the Display Board module.

ECT 4.754/1

Display Board Replacement

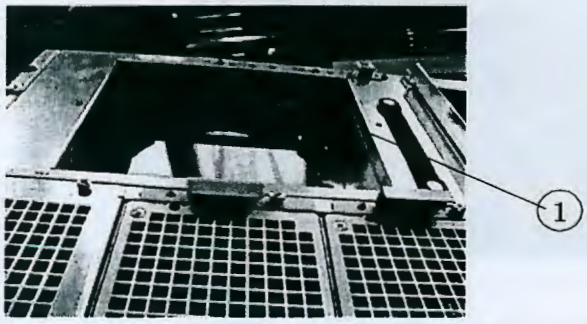
The Display Board contains the server's ON/OFF switch and five LEDs that indicate server status when power is applied.

CAUTION The Display Board is not a HotSwap or HotPlug unit. Ensure that it is powered-down prior to removal.

To replace the Display Board, perform the following tasks:

1. Reconnect the ribbon cable to the Display Board.
2. Carefully push the Display Board up through the top of the Chassis Fan cavity and insert the LEDs and On/Off switch into their respective chassis openings.
3. Replace three T-10 screws.

The following graphic shows the Display Board location (item 1) (looking up from the bottom of the front of the server).



The next graphic shows the Display Board module.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1639
Fls:
Doc: 3701

Platform Monitor Removal

The Platform Monitor resides on the System Board and is accessed via the Top Service Bay.

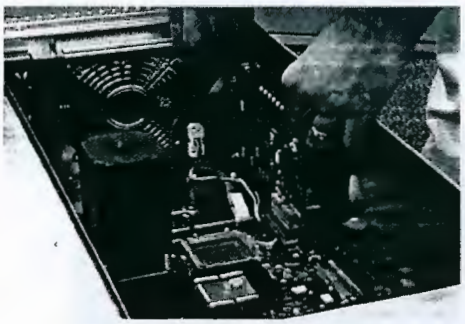
Removing rp5400 and/or rp5450 Model Platform Monitors

Looking into the Top Service Bay from the front, the rp5400/rp5450 model Platform Monitor is located on the left side at the front of the server.

To remove the rp5400/rp5450 model Platform Monitor, perform the following steps:

1. Pull up on the extractor levers on each end of the Platform Monitor to unseat it from its socket.
2. When the Platform Monitor unseats from the socket, pull it up and away from the System Board.

The following graphics show a Platform Monitor board followed by a display of Platform Monitor removal/replacement.



Removing The rp5470 Model Platform Monitor

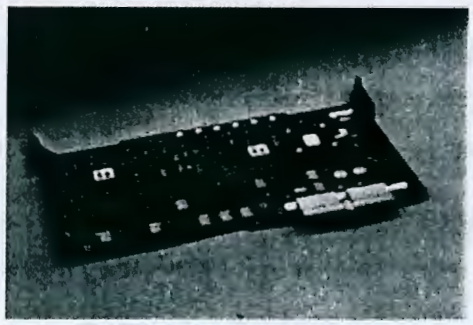
Looking into the Top Service Bay from the front, the rp5470 model Platform Monitor is located on the right side at the front of the server.

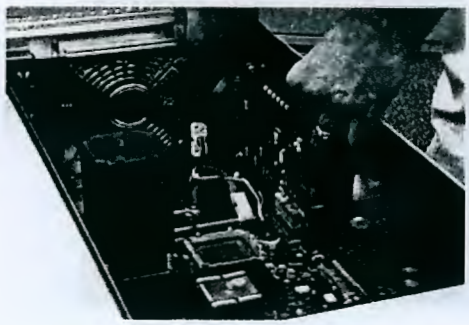
To remove an rp5470 model Platform Monitor, perform the following steps:

1. Pull up on the extractor levers on each end of the Platform Monitor to unseat it from its socket.
2. When the Platform Monitor unseats from the socket, pull it up and away from the System Board.

E C T
4.7521
U
AC

The following graphics show a Platform Monitor board followed by a display of Platform Monitor removal/replacement.





RQS Nº 03/2005 - CN
CPMI - CORREIOS
1640
Fls:
3701
Doc:

Platform Monitor Replacement

The Platform Monitor resides on the System Board and is accessed via the Top Service Bay.

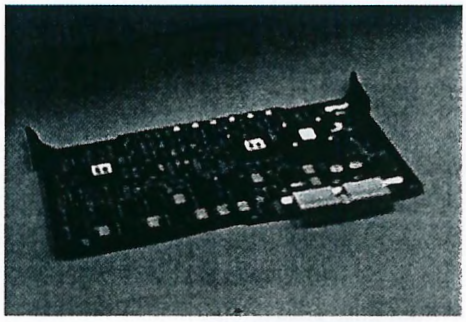
Replacing rp5400 and/or rp5450 Platform Monitors

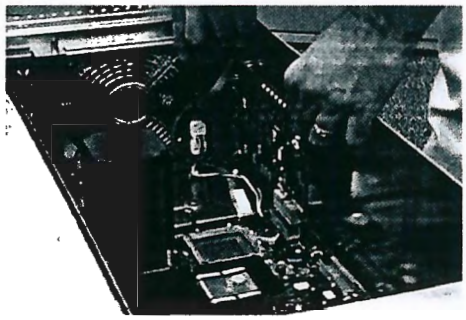
Looking into the Top Service Bay from the front, the rp5400/rp5450 model Platform Monitor is located on the left side at the front of the server.

To replace a Platform Monitor, perform the following steps:

1. Seat the Platform Monitor into its socket.
2. Lift the extractor levers and press them onto each end of the Platform Monitor until the levers snap into place.

The following graphics show a Platform Monitor board followed by a display of Platform Monitor removal/replacement.





Replacing rp5470 Platform Monitor

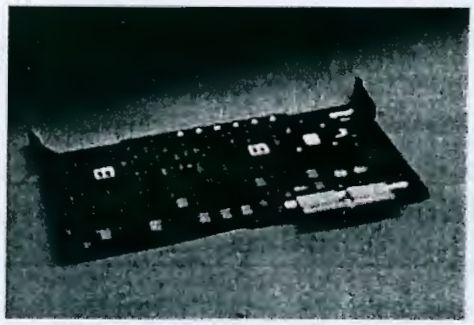
Looking into the Top Service Bay from the front, the rp5470 model Platform Monitor is located on the right side at the front of the server.

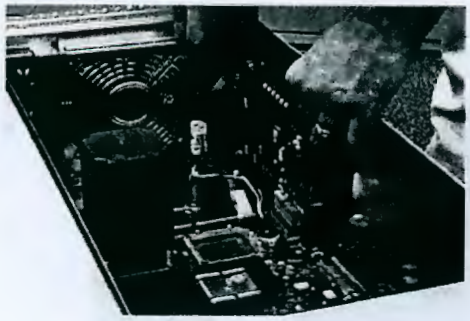
To replace a Platform Monitor, perform the following steps:

1. Seat the Platform Monitor into its socket.
2. Lift the extractor levers and press them onto each end of the Platform Monitor until the levers snap into place.

E C T
4.750
C R L - A C

The following graphics show a Platform Monitor board followed by a display of Platform Monitor removal/replacement.





RQS Nº 03/2005 - CN
CPMI - CORREIOS
1641
Fls:
3701
Doc:

PCI I/O Card Removal

The side service bay contains card slots for ten PCI I/O cards (slots 3 through 12) and two Core I/O cards (slots 1 and 2).

Perform the following tasks prior to removing PCI I/O cards:

- Power down the server.
- Detach all power cords from the server.

To remove a PCI I/O card from the server, perform the following steps:

NOTE Record the location of all PCI cards as they are removed. Replacing them in a diffferent location will require system reconfiguration and could cause boot failure.

---

1. Disconnect the I/O cable attached to the I/O card at the rear PCI bulkhead.
2. Disconnect any ribbon cable connectors attached to the I/O card in the side service bay.
3. Grasp the edge of the I/O card and pull it out of the server.

The following graphic shows an I/O card being removed.

PCI I/O Card Replacement

The side service bay contains card slots for 10 PCI I/O cards (slots 3 through 12) and 2 Core I/O cards (slots 1 and 2).

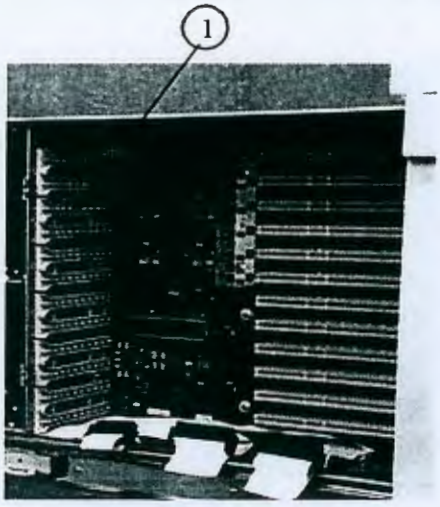
Prior to replacing PCI cards, perform the steps listed below:

- Power down the server.
- Detach all power cords from the server.

To replace a Core or PCI I/O card, perform the following steps:

1. Locate the I/O card guide (item 1) on the outside of the Fan Assembly Housing. Orient the I/O card into its guide slot and push it into the server until the card connector seats in the I/O Backplane card connector.

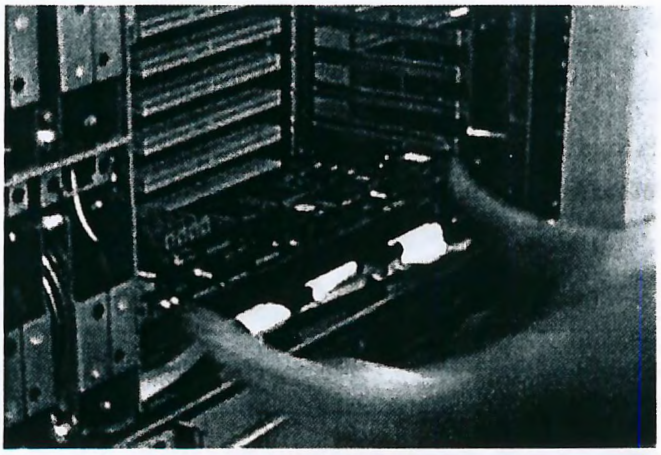
NOTE Each I/O card guide contains two slots. The top slot is aligned with the I/O Backplane card connector.



2. Connect the I/O cable attached to the I/O card at the rear PCI bulkhead.
3. Connect any ribbon cable connectors attached to the I/O card in the side service bay.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1642
Fls:
3701
Doc:

The following graphic shows an I/O card being replaced.



ECT
4.746
1
AC

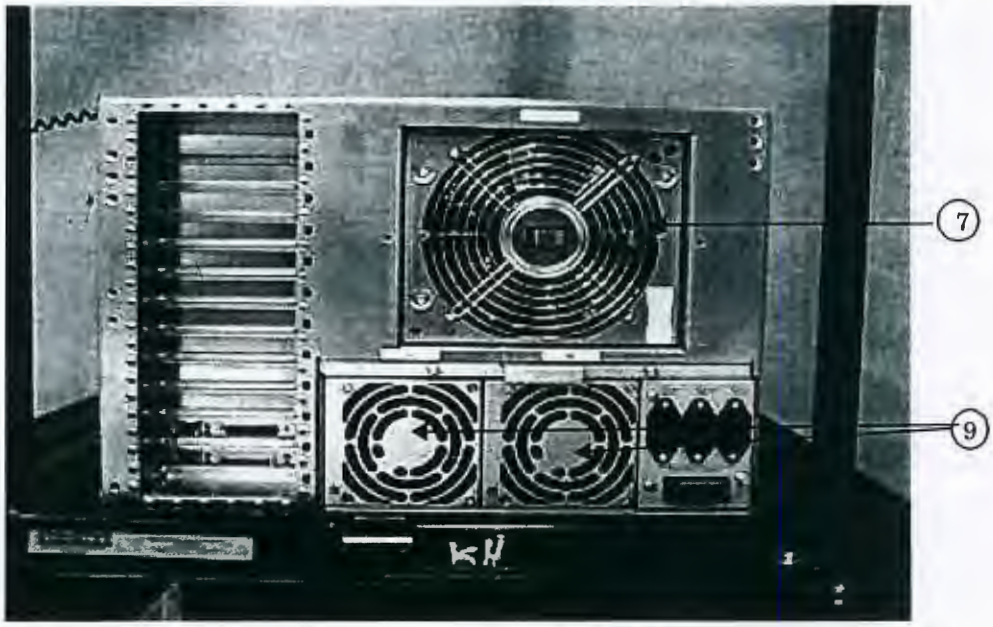
A Parts and Accessories

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1643
Fls:
3701
Doc:

CRU Physical Location

This section contains views of the rp54xx computer. The locator numbers in the diagrams correspond to the numbers in the CRU Part Number section.

Figure A-1 Server Rear View



ECT
Parts and Accessories
CRU Physical Location
CPL - ACJ

Figure A-2 Side Service Bay

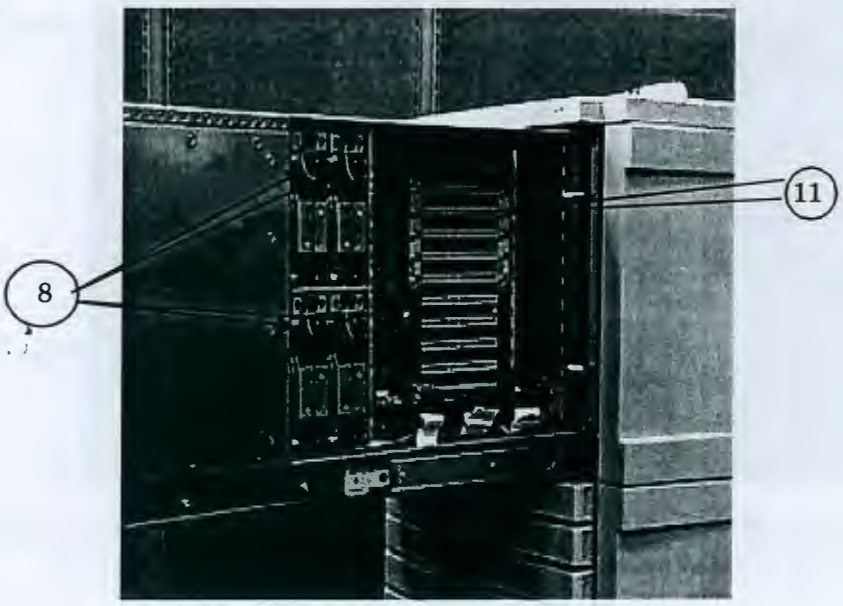
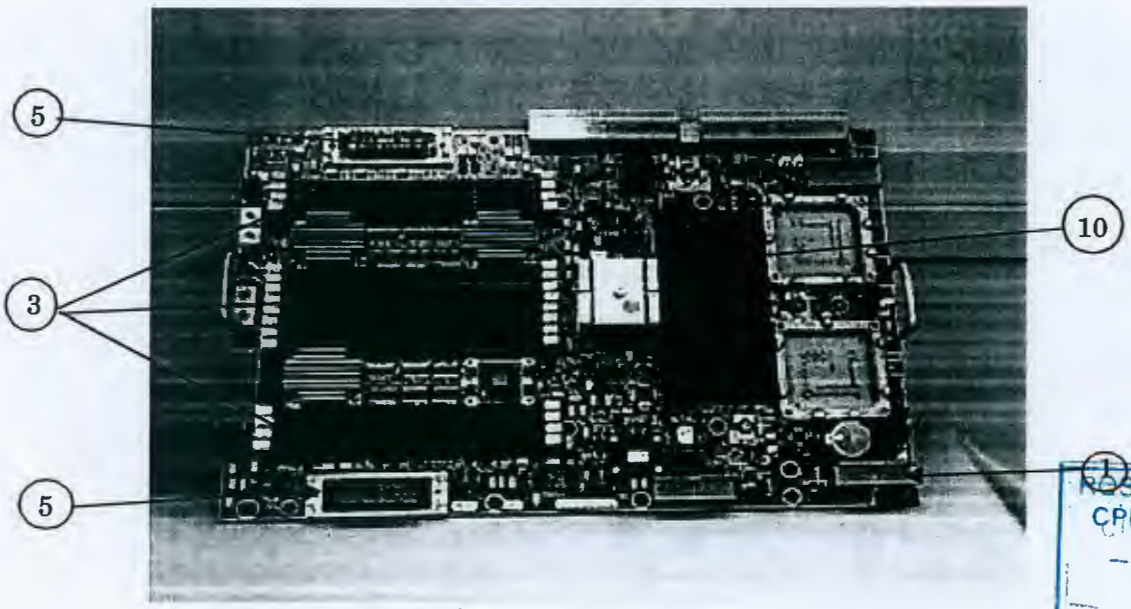
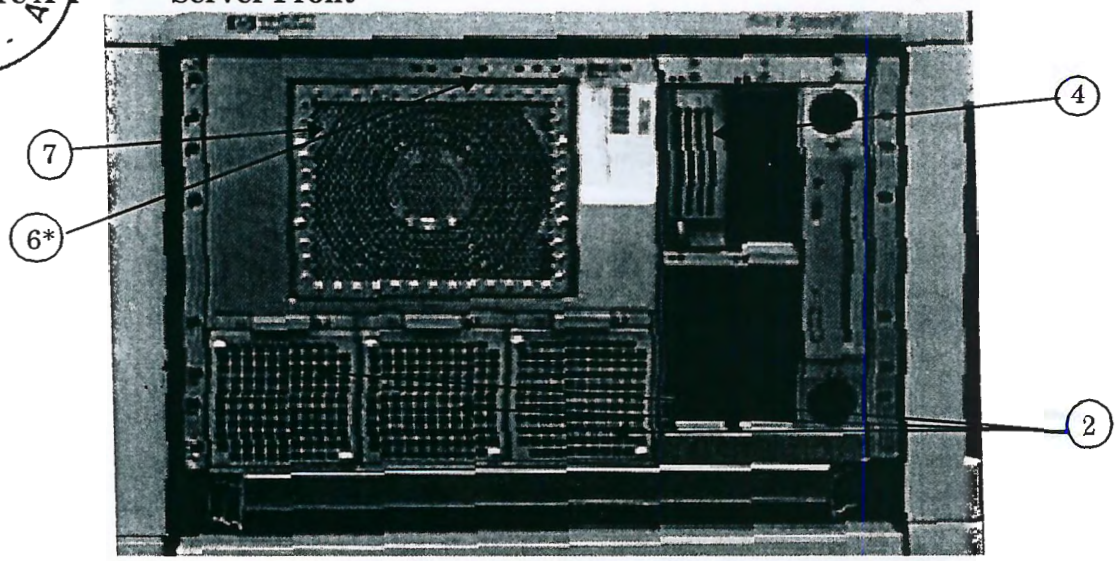


Figure A-3 System Board (Access via Top Service Bay)



ROS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1644
Doc: 3701

Figure A-4 Server Front



*The Display Board is accessed by removing the Chassis Fan screen and fan (item 7). The Display Board is located through a slot in the inside top of the Chassis Fan cavity.

4.742 1
J
AC

Customer Replaceable Unit Part Numbers

The following tables list all Customer Replaceable Units (CRUs) for the rp54xx computer system. The following tables list both new and exchange part numbers.

Table A-1 Exchange CRUs

Product #	New Part #	Exch. Part #	Description	Loc #
A5191A/B A5576A/B A6144A/B A6797B	A5191-60010	A5191-69010	Platform Monitor Board	1
A5527A	0950-3471	A5527-69001	Power Supply	2
A6155A	A6155-60001	A6155-69001	Memory Carrier	NA
A6115A	A6115-60001	A6115-69001	1024 MB Memory DIMM	3
A5798A	A5798-60001	A5798-69001	512 MB Memory DIMM	
A5797A	A5797-60001	A5797-69001	256 MB Memory DIMM	
A5554A	A5554-60002	A5554-69002	128 MB Memory DIMM	
A5802A	A5802-67001	A5802-69001	9 GB HotPlug Disk Assembly	4
A5803A	A5803-67001	A5803-69001	18 GB HotPlug Disk Assembly	
A6110A	A6110-67001	A6110-69001	36 GB HotPlug Disk Assembly	
A5796A	A3639-60012	A3639-69012	PA-8500/8600 Processor Support Module	5
A6799A	0950-3908	A3639-69033	PA-8700 Processor Support Module	5
A6696A	A5191-60012	A5191-69012	Revision A GSP	NA
A6696B	A6144-60012	A6144-69012	Revision B GSP	NA

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1645
Doc: 3701

Table A-2 Non-Exchange CRUs

Product #	Part #	Description	Loc #
A5191A/B A5576A/B A6144A/B A6797B	A5191-60013	Display Board	6
	A5191-04002	Fan, Chassis (172m)	7
	A5191-04003	Fan, Card Cage (119m)	8
	A5191-67006	Fan, Power Converter	9
	0515-0664	Processor Cover Plate	10
	A5236-40024	Disk Filler Panel	NA
	A5191-00107	Power Supply Filler Panel	NA
	A3639-04024	PCI Separator/Extractor	11
A5576A/B A5191A/B A6144A	A5191-04008	Plastic Front Bezel, old style (split door)	NA
A5576A/B A5191A/B A6144A/B	A5191-04012[a]	Plastic Front Bezel, new style rp54xx (solid piece)	NA
A6797B	A5191-04013[a]	Plastic Front Bezel, rp54xx (solid piece)	NA
A5576A/B A5191A/B A6144A/B A6797B	A5191-70010	Bezel Hardware Kit	NA
A6696A	A5191-63001	W-Cable (beige color), use with revision A GSP (A5191-60012/69012) only	NA
A6696B	A6144-63001	M-Cable (black color), use with revision B GSP (A6144-60012/69012) only	NA

a. When replacing the split door bezel (A5191-04008) with a solid piece bezel, the Bezel Hardware Kit (A5191-70010) is required.

E C T
4.720
L - AC

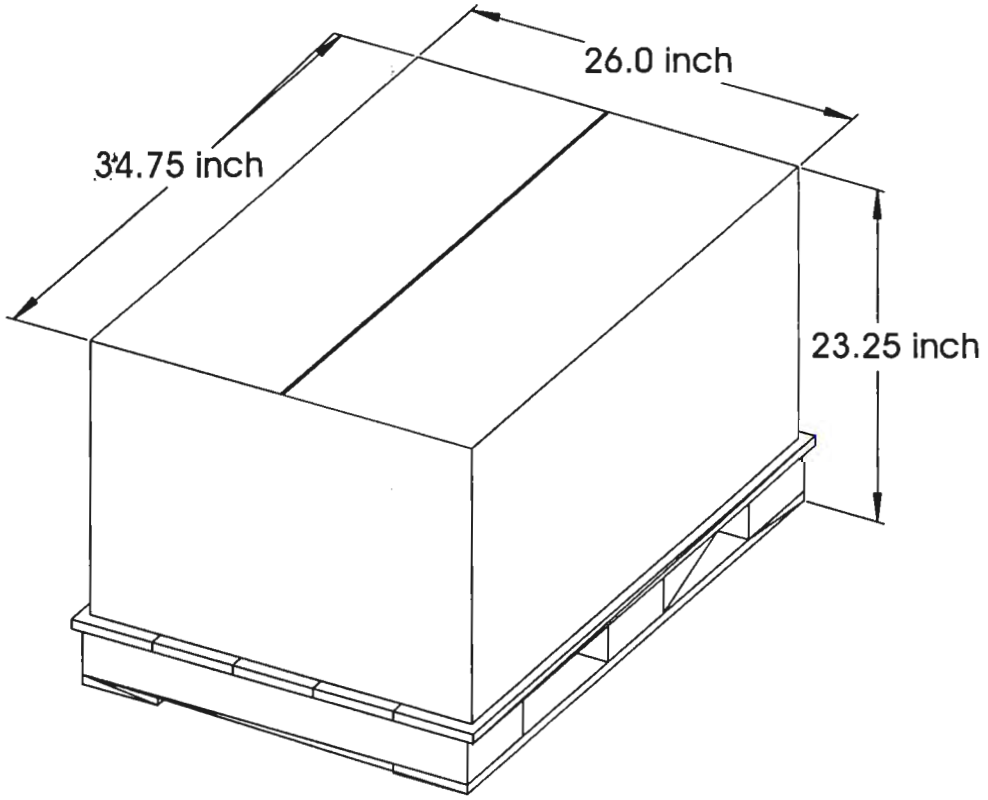
B System Specifications

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1646
Fls:
Doc: 3701

Dimensions

Uncrating Space

rp54xx systems are shipped in boxes on a 34.75 in. x 26 in. (88.25 cm. x 66 cm.) pallet. The combined height of the packaged container and the pallets is 23.25 in. (59 cm.).



rhrr004

Allow a circular area approximately 5 ft. (2 m.) in diameter room for uncrating the system. Allow additional space for temporary storage of the shipping containers and packing materials.

Space Requirements

A minimum access area of 2 ft. (0.7 m.) in all directions is required for serviceability.

ECT
4.738
1
3
L - AC

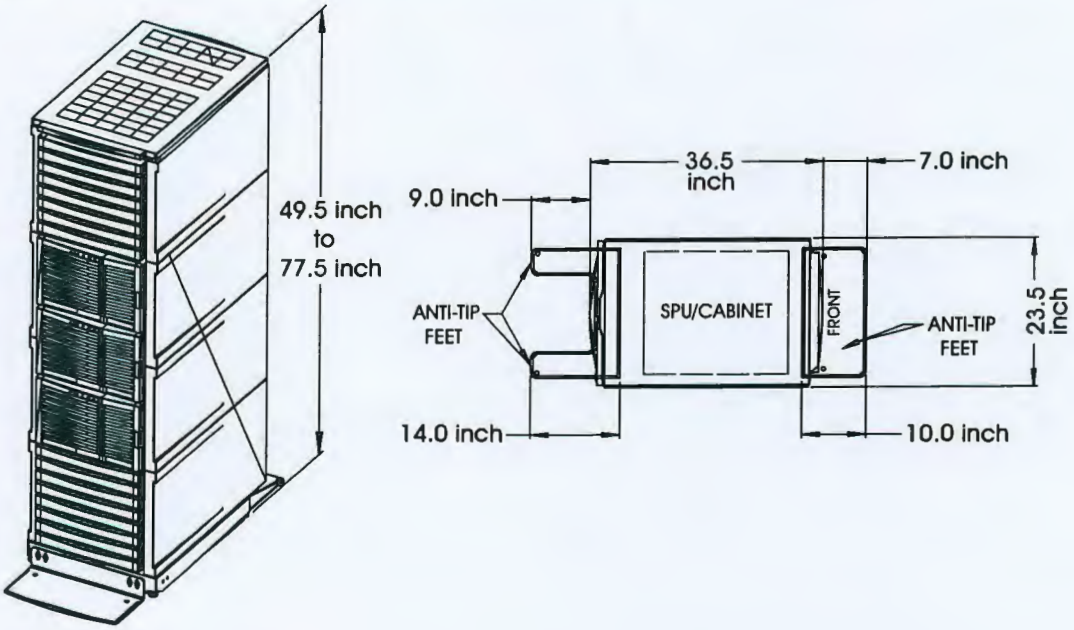
Computer Room Physical Space Requirements

Server

The A5537A, A5538A, or A5539A cabinets in which the server resides is 38.5" deep by 23.5" wide, with heights as follows:

- A5537A 1.2 meter rack - 49.5"
- A5538A 1.6 meter rack - 63.5"
- A5539A 2.0 meter rack - 77.5"

The cabinet anti-tip feet (required for safety) extend the depth an additional 10" in the front and 14" in the back. The minimum standalone physical space for the rp54xx server in a cabinet is shown in the following illustration:



rhrr005

For service access, the server slides on rails 28" beyond the edge of the chassis in the front. An additional minimum of 3' of workspace on all sides is required for servicing the server.

Aisle Space

The minimum aisle space between rows of installed HP rp54xx server/cabinets is 3 feet, front and back, for airflow and serviceability.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1647
Fls:
3701
Doc:

Computer Room Unpacking Space

Specify Uncrating Space

rp54xx Systems are shipped in integrated cabinets on a 34.75" (88.25 cm.) x 26" (66 cm.) pallet. The combined height of the packaged container and the pallets are as follows:

- 1.1 meter rack - 60 inches
- 1.6 meter rack - 73 inches
- 2.0 meter rack - 87 inches

Allow room (a circular area approximately 12 feet (3.5 meters) in diameter) for uncrating the system and rolling the cabinet off the pallet on rails. Allow additional space for temporary storage of the shipping containers and packing materials..

FACT
14.736
CPL - AC

Electrical

The HP rp54xx power system is comprised of one, two or three autoranging, 12A/10A/5A, 930W hot-swappable system power supplies, depending on how the system is configured. The maximum power needed by fully-configured server is 1200W. Each power supply requires a dedicated 20A branch circuit.

CAUTION HP does not recommend and does not support the use of "ferro-active" or "ferro-resonant" power correction in conjunction with the rp54xx server. These type of line conditioners represent an older technology that is not compatible with the most recent designs in active PFC power supplies such as those in the HP rp54xx servers. "Ferro-active" or "ferro-resonant" line conditioners may cause an increase in total harmonic distortion and may produce significant and unpredictable voltage regulation anomalies.

Office High Availability Requirements

Server-level Enhanced Power Availability

At the server level, enhanced power availability is achieved through the n+1 hot-swappable power supplies.

One power supply is required for a minimally configured rp54xx system operation and in order to allow the system to boot. If a second power supply is present, one of the two power supplies can fail without the system shutting down. Similarly, two power supplies are required for a more heavily-configured rp54xx server. If a third power supply is present, one of the two power supplies can fail without the system shutting down.

If a third (redundant) power supply is present, all three power supplies become hot-swappable. Any one of the power supplies can fail without affecting system performance, and can be replaced while the system is on-line. Single point of failure is reduced to the local wall circuit or PowerTrust UPS to which the power supply power cords are connected.

Power Protection

Power protection is provided through the use of HP PowerTrust UPSs (Uninterruptible Power Supplies). The only supported models for rp54xx systems are the 3.0kVA and 5.5kVA models. Recommendations for other manufacturers and models are not yet determined.

HP rp54xx server power supplies may be plugged directly into the customer's site UPS. However, customers are advised against plugging the power supply into an HP PowerTrust UPS and then connecting that UPS to the site UPS.

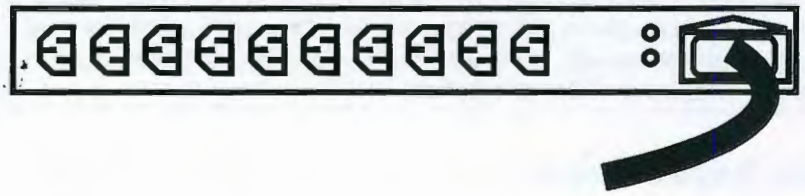
RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1648
Doc: 3701

Modular PDUs

NOTE The acronym PDU (Power Distribution Unit) in this document refers to the power strips attached to the HP rp54xx cabinet.

Three modular PDUs are available for use with the rp54xx product:

- 20A modular PDU, HP product number E7674A. This PDU has seven C13 outlets and one C19 outlet. Note that if this PDU is used to power the rp54xx server, any other peripherals must have their power supplied by additional PDUs in the cabinet. The PDU power cord (HP part number 8120-6903) has an L6-20P plug which must be plugged into an L6-20R wall or floor receptacle.



- 30A modular PDU, HP product number E7681A (North America) or E7682A (International). This PDU has eight C13 outlets and two C19 outlets, split across two 20A branch circuits (max. 30A available). The PDU power cord has an L6-30 plug.

- 60A modular PDU, HP product number E7683A (North America) or E7667A (International). FINAL DESIGN ON THIS PRODUCT IS NOT YET AVAILABLE.

System Power Requirements

Table B-1 Power Requirements

Requirements	Value	Comments
Nominal input voltage	100-240 VAC	
Frequency range (minimum - maximum)	50 - 60 HZ	
Number of phases	1	
Theoretical maximum current	12.0 A	Per line cord
Maximum inrush current	69.0 A	Per line cord
Ground leakage current (mA)	< 3.6 mA	Per line cord

E C T
4.734
J A C

LAN and Telephone

rp54xx servers provide remote console access via the secure web console, which may be connected to the RS-232 serial port or 10Base-T RJ45 LAN port on the GSP (Guardian Service Processor) card in I/O slot #2. The same connectors may also be used to connect directly to a hard console.

NOTE The RJ45 LAN port should be used ONLY for remote console access and not as a production LAN port.

rp54xx servers may require as many as three unique IP addresses:

- The rp54xx server requires its own IP address.
- The Guardian Service Processor, as a separate network device, has to have its own IP address, gateway, and subnet mask configured at the site in order to be separately addressed. The service processor does not support DHCP, so the IP address must be assigned out of a separate pool from any that are assigned dynamically.
- The remote web console, if used, requires its own IP address.

NOTE Check with your local telephone company to be thatsure the telephone service at the site can accommodate modem/data quality transmission.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1649
Fls:
3701
Doc:

Acoustic Safety Standards

The acoustic specifications for the rp54xx server are as follows:

Sound power	7.0 Bels LwA maximum at >31° C
Sound pressure	60 dB maximum at > 31° C
	No prominent tones

ECT
4.732
CPL - AC

Altitude Operation Standards

Maximum Altitude	
Operational	3000 meters above sea level
Non-operational	4572 meters above sea level

Effects of Altitude

Some old models of tape drives, including those supplied by Hewlett-Packard, have vacuum column transport mechanisms that are affected by atmospheric pressure. Adjustments to these mechanisms may be required to compensate for the lower atmospheric pressure at higher altitudes.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1650
Fls:
Doc: 3701

Temperature and Humidity Operating Standards

The following table lists the temperature and humidity specifications for rp54xx servers.

Temperature and Humidity Specifications				
Parameter	**Operational Limits**	**Recommended Operating Range**	**Maximum Rate of Change (per hour)**	**Non-Operating Ranges**
Temperature[a]	5°C to 35°C (41°F to 95°F)[b]	20°C to 25°C (68°F to 77°F)	10°C (50°F) per hour (With tape media) 20°C (68°F) per hour (Without tape media)	-40°C to +70°C (-40°F to +158°F)
Operating Humidity	15 to 80% Relative humidity (Non-condensing) at 35°C (95°F)	40 to 60% Relative humidity (Non-condensing)	30% Per hour Relative humidity (Non-condensing)	90% Relative humidity (Non-condensing) at 65°C (149°F)

a. The rp54xx has been designed to operate within the above specific temperature and relative humidity operational limits. In general, operating any electronic equipment within the recommended ranges of temperature and humidity will produce optimal reliability.
b. Temperature ranges stated above are at sea level. Maximum operating temperature is derated (reduced) by 2°C for each 1000 meters above sea level up to a maximum of 3000 meters.

NOTE Operating ranges refer to the ambient air temperature and humidity measured at the cabinet cooling air intake vents.

Thermal Protection Features

If the cabinet temperature approaches 35°C, thermal protection will be invoked. At 35°C +/- 2°C a warning message will be displayed on the system console. At 40°C +/- 2°C an ungraceful shutdown will occur.

E C T
4730
CPL - AC

C General Site Preparation Guidelines

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1651
Fls:
Doc: 3701

The following information provides general principles and practices to consider before the installation or operation of an hp server.

Electrical Factors

Proper design and installation of a power distribution system for an hp server requires specialized skills. Those responsible for this task must have a thorough knowledge and understanding of appropriate electrical codes and the limitations of the power systems for computer and data processing equipment.

In general, a well-designed power distribution system exceeds the requirements of most electrical codes. A good design, when coupled with proper installation practices, produces the most trouble-free operation.

A detailed discussion of power distribution system design and installation is beyond the scope of this information. However, electrical factors relating to power distribution system design and installation must be considered during the site preparation process.

The electrical factors discussed in this section are:

- Computer room safety
- Power Consumption
- Electrical load requirements (circuit breaker sizing)
- Power quality
- Distribution hardware
- System installation guidelines

Computer Room Safety

Inside the computer room, fire protection and adequate lighting (for equipment servicing) are important safety considerations. Federal and local safety codes govern computer installations.

Fire Protection

The National Fire Protection Association's Standard for the Protection of Electronic Computer Data Processing Equipment, NFPA 75, contains information on safety monitoring equipment for computer rooms.

Most computer room installations are equipped with the following fire protection devices:

- Smoke detectors
- Fire and temperature alarms
- Fire extinguishing system

Additional safety devices are:

- Circuit breakers
- An emergency power cutoff switch
- Devices specific to the geographic location i.e., earthquake protection

Lighting Requirements for Equipment Servicing

Adequate lighting and utility outlets in a computer room reduce the possibility of accidents during equipment servicing. Safer servicing is also more efficient and, therefore, less costly.

For example, adequate lighting reduces the chances of connector damage when cables are installed or removed.

ECT
4.728
FL - AC

The minimum recommended illumination level is 70 foot-candles (756 lumens per square meter) when the light level is measured at 30 inches (76.2 cm) above the floor.

Power Consumption

When determining power requirements, you must consider any peripheral equipment that will be installed during initial installation or as a later update. Refer to the applicable documentation for such devices to determine the power required to support these devices.

Electrical Load Requirements (Circuit Breaker Sizing)

NOTE Local authority has jurisdiction [LAHJ] and should make the final decision regarding adherence to country- specific electrical codes and guidelines.

It is good practice to derate power distribution systems for one or more of the following reasons:

- To avoid nuisance tripping from load shifts or power transients, circuit protection devices should never be run above 80% of their root-mean-square (RMS) current ratings.
- Safety agencies derate most power connectors to 80% of their RMS current ratings.

Power Quality

The hp server is designed to operate over a wide range of voltages and frequencies. The server is tested and shown to comply with EMC Specification EN50082. However, damage can occur if these ranges are exceeded. Severe electrical disturbances can exceed the design specifications of the equipment.

Sources of Voltage Fluctuations

Voltage fluctuations, sometimes called glitches, affect the quality of electrical power. Common sources of these disturbances are:

- Fluctuations occurring within the facility's distribution system
- Utility service low-voltage conditions (such as sags or brownouts)
- Wide and rapid variations in input voltage levels
- Wide and rapid variations in input power frequency
- Electrical storms
- Large inductive sources (such as motors and welders)
- Faults in the distribution system wiring (such as loose connections)
- Microwave, radar, radio, or cell phone transmissions

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1652
Fls:
Doc: 3701

Power System Protection

The hp server can be protected from the sources of many of these electrical disturbances by using:

- A dedicated power distribution system
- Power conditioning equipment
- Over- and under-voltage detection and protection circuits
- Screening to cancel out the effects of undesirable transmissions
- Lightning arresters on power cables to protect equipment against electrical storms

Precautions have been taken during power distribution system design to provide immunity to power outages of less than one cycle. However, testing cannot conclusively rule out loss of service. Therefore, adherence to the following guidelines provides the best possible performance of power distribution systems for hp computer equipment:

- Dedicated power source—Isolates an hp server power distribution system from other circuits in the facility.
- Missing-phase and low-voltage detectors—Shuts equipment down automatically when a severe power disruption occurs. For peripheral equipment, these devices are recommended but optional.
- Online uninterruptible power supply (UPS)—Keeps input voltage to devices constant and should be considered if outages of one-half cycle or more are common. Refer to qualified contractors or consultants for each situation.

Distribution Hardware

This section describes wire selection and the types of raceways (electrical conduits) used in the distribution system.

Wire Selection

Use copper conductors instead of aluminum, as aluminum's coefficient of expansion differs significantly from that of other metals used in power hardware. Because of this difference, aluminum conductors can cause connector hardware to work loose, overheat, and fail.

Raceway Systems (electrical conduits) [LAHJ]

Raceways (electrical conduits) form part of the protective ground path for personnel and equipment. Raceways protect the wiring from accidental damage and also provide a heatsink for the wires.

Any of the following types may be used:

- Electrical metallic tubing (EMT) thin-wall tubing
- Rigid (metal) conduit
- Liquidtight with RFI shield grounded (most commonly used under raised floors)

Building Distribution

All building feeders and branch circuitry should be in rigid metallic conduit with proper connectors (to provide ground continuity) Conduit that is exposed and subject to damage should be constructed of rigid galvanized steel.

ECT
4.726
CPL - AC

Grounding Systems

An hp server requires two methods of grounding:

- Power distribution safety grounding
- High frequency intercabinet grounding

Power Distribution Safety Grounding [LAHJ]

The power distribution safety grounding system consists of connecting various points in the power distribution system to earth ground using green (green/yellow) wire ground conductors. Having these ground connections tied to metal chassis parts that may be touched by computer room personnel protects them against shock hazard from current leakage and fault conditions.

Power distribution systems consist of several parts. Hewlett-Packard recommends that these parts be solidly interconnected to provide an equipotential ground to all points.

Main Building Electrical Ground The main electrical service entrance equipment should have an earth ground connection, as required by applicable codes. Connections such as a grounding rod, building steel, or a conductive type cold water service pipe provide an earth ground.

Electrical Conduit Ground All electrical conduits should be made of rigid metallic conduit that is securely connected together or bonded to panels and electrical boxes, so as to provide a continuous grounding system.

Power Panel Ground Each power panel should be grounded to the electrical service entrance with green (green/yellow) wire ground conductors. The green (green/yellow) wire ground conductors should be sized per applicable codes (based on circuit over current device ratings).

NOTE The green wire ground conductor mentioned above may be a black wire marked with green tape. [LAHJ]

Computer Safety Ground Ground all computer equipment with the green (green/yellow) wire included in the branch circuitry. The green (green/yellow) wire ground conductors should be connected to the appropriate power panel and should be sized per applicable codes (based on circuit over current device ratings).

Cabinet Performance Grounding (High Frequency Ground)

Signal interconnects between system cabinets require high frequency ground return paths. Connect all cabinets to site ground.

NOTE In some cases power distribution system green (green/yellow) wire ground conductors are too long and inductive to provide adequate high frequency ground return paths. Therefore, a ground strap (customer-supplied) should be used for connecting the system cabinet to the site grounding grid (customer-supplied). When connecting this ground, ensure that the raised floor is properly grounded for high frequency.

Power panels located in close proximity to the computer equipment should also be connected to the site grounding grid. Methods of providing a sufficiently high frequency ground grid are described in the next sections.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1653
Fls:
3701
Doc:

Raised Floor "High Frequency Noise" Grounding

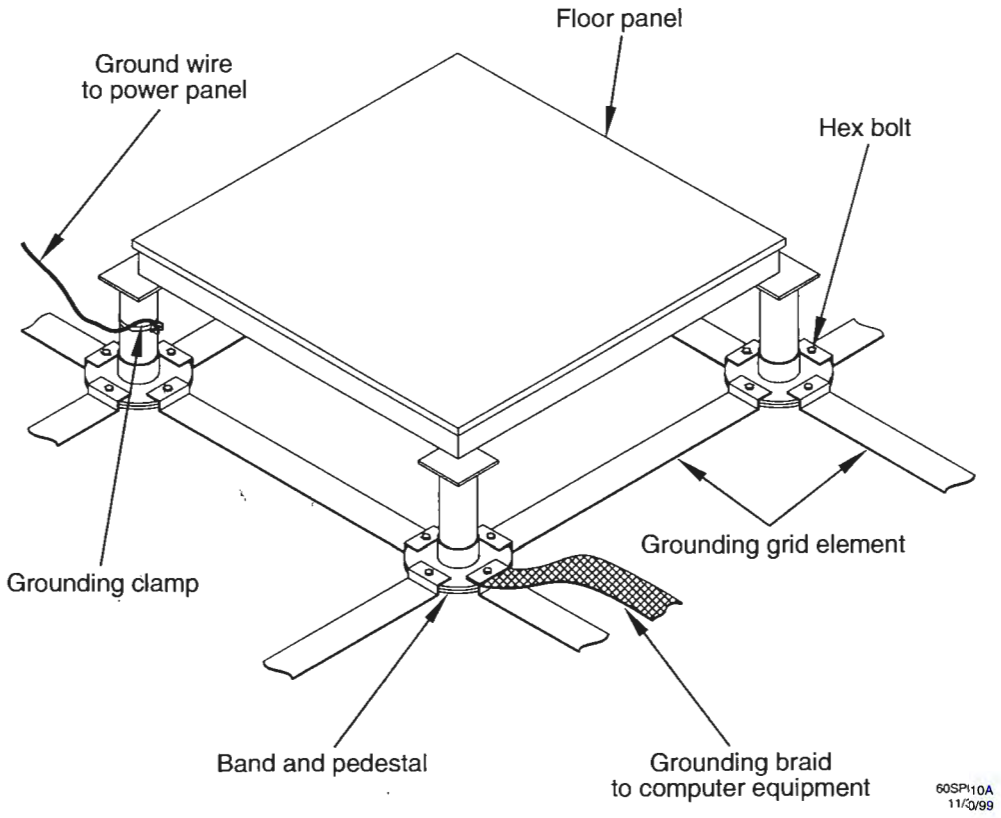
If a raised floor system is used, install a complete signal grounding grid for maintaining equal potential over a broad band of frequencies. The grounding grid should be connected to the equipment cabinet and electrical service entrance ground at multiple connection points using a minimum #6 AWG (16mm2) wire ground conductor. The following figure illustrates a metallic strip grounding system.

Hewlett-Packard recommends the following approaches:

- Excellent—Add a grounding grid to the subfloor. The grounding grid should be made of copper strips mounted to the subfloor. The strips should be 0.032 in. (0.08 cm) thick and a minimum of 3.0 in. (8.0 cm) wide.

  Connect each pedestal to four strips using 1/4 in. (6.0 mm) bolts tightened to the manufacturer's torque recommendation.
- Better - A grounded #6 AWG minimum copper wire grid mechanically clamped to floor pedestals and properly bonded to the building/site ground.
- Good—Use the raised floor structure as a ground grid. In this case, the floor must be designed as a ground grid with bolted down stringers and corrosion resistive plating (to provide low resistance and attachment points for connection to service entrance ground and hp computer equipment). The use of conductive floor tiles with this style of grid further enhances ground performance.

Figure C-1 Raised Floor Metal Strip Ground System



ECT 14.724 J CPL - AC

Equipment Grounding Implementation Details

Connect all Hewlett-Packard equipment cabinets to the site ground grid as follows:

Step 1. Attach one end of each ground strap to the applicable cabinet ground lug.

Step 2. Attach the other end to the nearest pedestal base (raised floor) or cable trough ground point (nonraised floor).

Step 3. Check that the braid contact on each end of the ground strap consists of a terminal and connection hardware (a 1/4-in. (6.0-mm) bolt, nuts, and washers).

Step 4. Check that the braid contact connection points are free of paint or other insulating material and treated with a contact enhancement compound (similar to Burndy Penetrox).

System Installation Guidelines

This section contains information about installation practices. Some common pitfalls are highlighted. Both power cable and data communications cable installations are discussed.

NOTE In domestic installations, the proper receptacles should be installed prior to the arrival of Hewlett-Packard equipment. Refer to the appropriate installation guide for installation procedures.

Wiring Connections

Expansion and contraction rates vary among different metals. Therefore, the integrity of an electrical connection depends on the restraining force applied. Connections that are too tight compress or deform the hardware and causes it to weaken. This usually leads to high impedance preventing circuit breakers from tripping when needed or can contribute to a buildup of high frequency noise.

CAUTION Connections that are too loose or too tight can have a high impedance that cause serious problems, such as erratic equipment operation. A high impedance connection overheats and sometimes causes fire or high temperatures that can destroy hard-to-replace components such as distribution panels or system bus bars.

Wiring connections must be properly torqued. Many equipment manufacturers specify the proper connection torque values for their hardware.

Ground connections must only be made on a conductive, nonpainted surface. When equipment vibration is present, lock washers must be used on all connections to prevent connection hardware from working loose.

Data Communications Cables

Power transformers create high-energy fields in the form of electromagnetic interference (EMI). Heavy foot traffic can create electrostatic discharge (ESD) that can damage electronic components. Route data communications cables away from these areas. Use shielded data communications cables that meet approved industry standards to reduce the effects of external fields.

PROS Nº 03/2005 - CN
CPMI - CORREIOS
1654
Fls:
Doc: 3701

Environmental Elements

The following environmental elements can affect an hp server installation:

- Computer room preparation
- Cooling requirements
- Humidity level
- Air conditioning ducts
- Dust and pollution control
- Electrostatic discharge (ESD) prevention
- Acoustics (noise reduction)

Computer Room Preparation

The following guidelines are recommended when preparing a computer room for an hp server:

- Locate the computer room away from the exterior walls of the building to avoid the heat gain from windows and exterior wall surfaces.
- When exterior windows are unavoidable, use windows that are double or triple glazed and shaded to prevent direct sunlight from entering the computer room.
- Maintain the computer room at a positive pressure relative to surrounding spaces.
- Use a vapor barrier installed around the entire computer room envelope to restrain moisture migration.
- Caulk and vapor seal all pipes and cables that penetrate the envelope.
- Use at least a 12-inch raised floor system for minimum favorable room air distribution system (underfloor distribution).
- Ensure a minimum clearance of 12 inches between the top of the hp server cabinet and the ceiling to allow for return air flow and ensure that all ceiling tiles are in place.
- Allow 18 inches (or local code minimum clearance) from the top of the hp server cabinet to the fire sprinkler heads.

Cooling Requirements

Air conditioning equipment requirements and recommendations are described in the following sections.

Basic Air Conditioning Equipment Requirements

The cooling capacity of the installed air conditioning equipment for the computer room should be sufficient to offset the computer equipment dissipation loads, as well as any space envelope heat gain. This equipment should include:

- Air filtration
- Cooling or dehumidification
- Humidification
- Reheating

ECT 4.726 J CPL - AC

Grounding Systems

An hp server requires two methods of grounding:

- Power distribution safety grounding
- High frequency intercabinet grounding

Power Distribution Safety Grounding [LAHJ]

The power distribution safety grounding system consists of connecting various points in the power distribution system to earth ground using green (green/yellow) wire ground conductors. Having these ground connections tied to metal chassis parts that may be touched by computer room personnel protects them against shock hazard from current leakage and fault conditions.

Power distribution systems consist of several parts. Hewlett-Packard recommends that these parts be solidly interconnected to provide an equipotential ground to all points.

Main Building Electrical Ground The main electrical service entrance equipment should have an earth ground connection, as required by applicable codes. Connections such as a grounding rod, building steel, or a conductive type cold water service pipe provide an earth ground.

Electrical Conduit Ground All electrical conduits should be made of rigid metallic conduit that is securely connected together or bonded to panels and electrical boxes, so as to provide a continuous grounding system.

Power Panel Ground Each power panel should be grounded to the electrical service entrance with green (green/yellow) wire ground conductors. The green (green/yellow) wire ground conductors should be sized per applicable codes (based on circuit over current device ratings).

NOTE The green wire ground conductor mentioned above may be a black wire marked with green tape. [LAHJ]

Computer Safety Ground Ground all computer equipment with the green (green/yellow) wire included in the branch circuitry. The green (green/yellow) wire ground conductors should be connected to the appropriate power panel and should be sized per applicable codes (based on circuit over current device ratings).

Cabinet Performance Grounding (High Frequency Ground)

Signal interconnects between system cabinets require high frequency ground return paths. Connect all cabinets to site ground.

NOTE In some cases power distribution system green (green/yellow) wire ground conductors are too long and inductive to provide adequate high frequency ground return paths. Therefore, a ground strap (customer-supplied) should be used for connecting the system cabinet to the site grounding grid (customer-supplied). When connecting this ground, ensure that the raised floor is properly grounded for high frequency.

Power panels located in close proximity to the computer equipment should also be connected to the site grounding grid. Methods of providing a sufficiently high frequency ground grid are described in the next sections.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1655
Fls:
3701
Doc:

Raised Floor "High Frequency Noise" Grounding

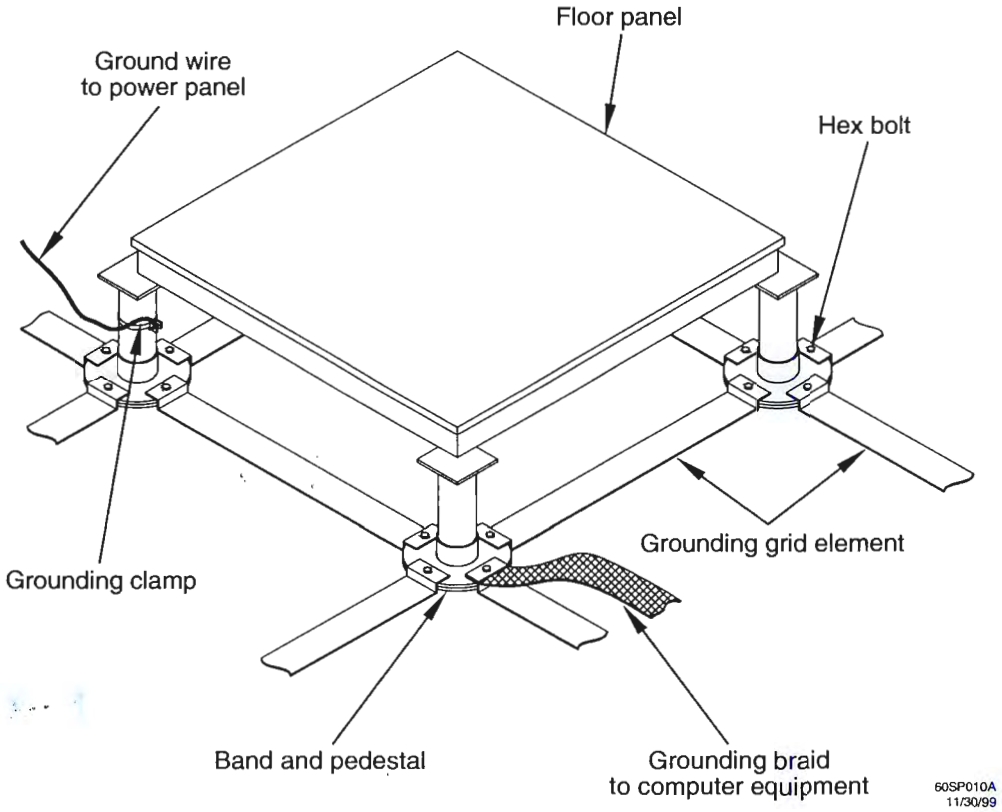
If a raised floor system is used, install a complete signal grounding grid for maintaining equal potential over a broad band of frequencies. The grounding grid should be connected to the equipment cabinet and electrical service entrance ground at multiple connection points using a minimum #6 AWG (16mm2) wire ground conductor. The following figure illustrates a metallic strip grounding system.

Hewlett-Packard recommends the following approaches:

- Excellent—Add a grounding grid to the subfloor. The grounding grid should be made of copper strips mounted to the subfloor. The strips should be 0.032 in. (0.08 cm) thick and a minimum of 3.0 in. (8.0 cm) wide.

  Connect each pedestal to four strips using 1/4 in. (6.0 mm) bolts tightened to the manufacturer's torque recommendation.
- Better - A grounded #6 AWG minimum copper wire grid mechanically clamped to floor pedestals and properly bonded to the building/site ground.
- Good—Use the raised floor structure as a ground grid. In this case, the floor must be designed as a ground grid with bolted down stringers and corrosion resistive plating (to provide low resistance and attachment points for connection to service entrance ground and hp computer equipment). The use of conductive floor tiles with this style of grid further enhances ground performance.

Figure C-1 Raised Floor Metal Strip Ground System



ECT
14.724
CPL - AC

Equipment Grounding Implementation Details

Connect all Hewlett-Packard equipment cabinets to the site ground grid as follows:

Step 1. Attach one end of each ground strap to the applicable cabinet ground lug.

Step 2. Attach the other end to the nearest pedestal base (raised floor) or cable trough ground point (nonraised floor).

Step 3. Check that the braid contact on each end of the ground strap consists of a terminal and connection hardware (a 1/4-in. (6.0-mm) bolt, nuts, and washers).

Step 4. Check that the braid contact connection points are free of paint or other insulating material and treated with a contact enhancement compound (similar to Burndy Penetrox).

System Installation Guidelines

This section contains information about installation practices. Some common pitfalls are highlighted. Both power cable and data communications cable installations are discussed.

NOTE In domestic installations, the proper receptacles should be installed prior to the arrival of Hewlett-Packard equipment. Refer to the appropriate installation guide for installation procedures.

Wiring Connections

Expansion and contraction rates vary among different metals. Therefore, the integrity of an electrical connection depends on the restraining force applied. Connections that are too tight compress or deform the hardware and causes it to weaken. This usually leads to high impedance preventing circuit breakers from tripping when needed or can contribute to a buildup of high frequency noise.

CAUTION Connections that are too loose or too tight can have a high impedance that cause serious problems, such as erratic equipment operation. A high impedance connection overheats and sometimes causes fire or high temperatures that can destroy hard-to-replace components such as distribution panels or system bus bars.

Wiring connections must be properly torqued. Many equipment manufacturers specify the proper connection torque values for their hardware.

Ground connections must only be made on a conductive, nonpainted surface. When equipment vibration is present, lock washers must be used on all connections to prevent connection hardware from working loose.

Data Communications Cables

Power transformers create high-energy fields in the form of electromagnetic interference (EMI). Heavy foot traffic can create electrostatic discharge (ESD) that can damage electronic components. Route data communications cables away from these areas. Use shielded data communications cables that meet approved industry standards to reduce the effects of external fields.

RQS nº 03/2005 - CN
CPMI - CORREIOS
1656
Fls:
3701
Doc:

Environmental Elements

The following environmental elements can affect an hp server installation:

- Computer room preparation
- Cooling requirements
- Humidity level
- Air conditioning ducts
- Dust and pollution control
- Electrostatic discharge (ESD) prevention
- Acoustics (noise reduction)

Computer Room Preparation

The following guidelines are recommended when preparing a computer room for an hp server:

- Locate the computer room away from the exterior walls of the building to avoid the heat gain from windows and exterior wall surfaces.
- When exterior windows are unavoidable, use windows that are double or triple glazed and shaded to prevent direct sunlight from entering the computer room.
- Maintain the computer room at a positive pressure relative to surrounding spaces.
- Use a vapor barrier installed around the entire computer room envelope to restrain moisture migration.
- Caulk and vapor seal all pipes and cables that penetrate the envelope.
- Use at least a 12-inch raised floor system for minimum favorable room air distribution system (underfloor distribution).
- Ensure a minimum clearance of 12 inches between the top of the hp server cabinet and the ceiling to allow for return air flow and ensure that all ceiling tiles are in place.
- Allow 18 inches (or local code minimum clearance) from the top of the hp server cabinet to the fire sprinkler heads.

Cooling Requirements

Air conditioning equipment requirements and recommendations are described in the following sections.

Basic Air Conditioning Equipment Requirements

The cooling capacity of the installed air conditioning equipment for the computer room should be sufficient to offset the computer equipment dissipation loads, as well as any space envelope heat gain. This equipment should include:

- Air filtration
- Cooling or dehumidification
- Humidification
- Reheating

EC
4.722
CPL AC

- Air distribution
- System controls adequate to maintain the computer room within specified operating ranges.

Lighting and personnel must also be included. For example, a person dissipates about 450 BTUs per hour while performing a typical computer room task.

At altitudes above 10,000 feet (3048 m), the lower air density reduces the cooling capability of air conditioning systems. If your facility is located above this altitude, the recommended temperature ranges may need to be modified. For each 1000 feet (305 m) increase in altitude above 10,000 feet (up to a maximum of 15,000 feet), subtract 1.5° F (0.83° C) from the upper limit of the temperature range.

Air Conditioning System Guidelines

The following guidelines are recommended when designing an air conditioning system and selecting the necessary equipment:

- The air conditioning system that serves the computer room should be capable of operating 24 hours a day, 365 days a year. It should also be independent of other systems in the building.
- Consider the long-term value of hp server availability, redundant air conditioning equipment or capacity.
- The system should be capable of handling any future hp server expansion.
- Air conditioning equipment air filters should have a minimum rating of 45% (based on "ASHRAE Standard 52-76, Dust Spot Efficiency Test").
- Introduce only enough outside air into the system to meet building code requirements (for human occupancy) and to maintain a positive air pressure in the computer room.

Air Conditioning System Types

The following three air conditioning system types are listed in order of preference:

- Complete self-contained package unit(s) with remote condenser(s). These systems are available with up or down discharge and are usually located in the computer room.
- Chilled water package unit with remote chilled water plant. These systems are available with up or down discharge and are usually located in the computer room.
- Central station air handling units with remote refrigeration equipment. These systems are usually located outside the computer room.

Basic Air Distribution Systems

A basic air distribution system includes supply air and return air.

An air distribution system should be zoned to deliver an adequate amount of supply air to the cooling air intake vents of the hp server equipment cabinets. Supply air temperature should be maintained within the following parameters:

- Ceiling supply system—From 55° F (12.8° C) to 60° F (15.6° C)
- Floor supply system—At least 60° F (15.6° C)

If a ceiling plenum return air system or a ducted ceiling return air system is used, the return air grill(s) in the ceiling should be above the exhaust area or the exhaust row.

The following three types of air distribution system are listed in order of recommendation:

- Underfloor air distribution system—Downflow air conditioning equipment located on the raised floor of the computer room uses the cavity beneath the raised floor as plenum for the supply air.

ROS Nº 03/2005 - CIN
CPMI - CORREIOS
1657
3701
Doc:

Perforated floor panels (available from the raised floor manufacturer) should be located around the front of the system cabinets. Supply air emitted though the perforated floor panels is then available near the cooling air intake vents of the hp server cabinets.

- Ceiling plenum air distribution system—Supply air is ducted into the ceiling plenum from upflow air conditioning equipment located in the computer room or from an air handling unit (remote).

  The ceiling construction should resist air leakage. Place perforated ceiling panels (with down discharge air flow characteristics) around the front of the system cabinets. The supply air emitted downward from the perforated ceiling panels is then available near the cooling air intake vents of the hp server cabinets.

  Return air should be ducted back to the air conditioning equipment though the return air duct above the ceiling.

- Above ceiling ducted air distribution system—Supply air is ducted into a ceiling diffuser system from upflow air conditioning equipment located in the computer room or from an air handling unit (remote).

  Adjust the supply air diffuser system grilles to direct the cooling air downward around the front of the hp server cabinets. The supply air is then available near the cooling air intake vents of the hp server cabinets.

Air Conditioning System Installation

All air conditioning equipment, materials, and installation must comply with any applicable construction codes. Installation of the various components of the air conditioning system must also conform to the air conditioning equipment manufacturer's recommendations.

Air Conditioning Ducts

Use separate computer room air conditioning duct work. If it is not separate from the rest of the building, it might be difficult to control cooling and air pressure levels. Duct work seals are important for maintaining a balanced air conditioning system and high static air pressure. Adequate cooling capacity means little if the direction and rate of air flow cannot be controlled because of poor duct sealing. Also, the ducts should not be exposed to warm air, or humidity levels may increase.

Humidity Level

Maintain proper humidity levels at 40 to 60% RH. High humidity causes galvanic actions to occur between some dissimilar metals. This eventually causes a high resistance between connections, leading to equipment failures. High humidity can also have an adverse affect on some magnetic tapes and paper media.

CAUTION Low humidity contributes to undesirably high levels of electrostatic charges. This increases the electrostatic discharge (ESD) voltage potential. ESD can cause component damage during servicing operations. Paper feed problems on high-speed printers are usually encountered in low-humidity environments.

Low humidity levels are often the result of the facility heating system and occur during the cold season. Most heating systems cause air to have a low humidity level, unless the system has a built-in humidifier.

Dust and Pollution Control

Computer equipment can be adversely affected by dust and microscopic particles in the site environment.

Specifically, disk drives, tape drives, and some other mechanical devices can have bearing failures resulting from airborne abrasive particles. Dust may also blanket electronic components like printed circuit boards causing premature failure due to excess heat and/or humidity build up on the boards. Other failures to power

supplies and other electronic components can be caused by metallically conductive particles, including zinc whiskers. These metallic particles are conductive and can short circuit electronic components. Use every effort to ensure that the environment is as dust and particulate free as possible. See the following heading titled "Metallic Particulate Contamination" for additional details.

Smaller particles can pass though some filters and over a period of time, cause problems in mechanical parts. Small dust particles can be prevented from entering the computer room by maintaining the air conditioning system at a high static air pressure level.

Other sources of dust, metallic, conductive, abrasive, and/or microscopic particles can be present. Some sources of these particulates are:

- Subfloor shedding
- Raised floor shedding
- Ceiling tile shedding

These particulates are not always visible to the naked eye. A good check to determine their possible presence is to check the underside of the tiles. The tile should be shiny, galvanized, and free from rust.

The computer room should be kept clean. The following guidelines are recommended:

- Smoking—Establish a no-smoking policy. Cigarette smoke particles are eight times larger than the clearance between disk drive read/write heads and the disk surface.
- Printer—Locate printers and paper products in a separate room to eliminate paper particulate problems.
- Eating or drinking—Establish a no-eating or drinking policy. Spilled liquids can cause short circuits in equipment such as keyboards.
- Tile floors—Use a dust-absorbent cloth mop rather than a dry mop to clean tile floors.

Special precautions are necessary if the computer room is near a source of air pollution. Some air pollutants, especially hydrogen sulfide (H2S), are not only unpleasant but corrosive as well. Hydrogen sulfide damages wiring and delicate sound equipment. The use of activated charcoal filters reduces this form of air pollution.

Metallic Particulate Contamination

Metallic particulates can be especially harmful around electronic equipment. This type of contamination may enter the data center environment from a variety of sources, including but not limited to raised floor tiles, worn air conditioning parts, heating ducts, rotor brushes in vacuum cleaners or printer component wear. Because metallic particulates conduct electricity, they have an increased potential for creating short circuits in electronic equipment. This problem is exaggerated by the increasingly dense circuitry of electronic equipment.

Over time, very fine whiskers of pure metal can form on electroplated zinc, cadmium, or tin surfaces. If these whiskers are disturbed, they may break off and become airborne, possibly causing failures or operational interruptions. For over 50 years, the electronics industry has been aware of the relatively rare but possible threat posed by metallic particulate contamination. During recent years, a growing concern has developed in computer rooms where these conductive contaminants are formed on the bottom of some raised floor tiles.

Although this problem is relatively rare, it may be an issue within your computer room. Since metallic contamination can cause permanent or intermittent failures on your electronic equipment, Hewlett-Packard strongly recommends that your site be evaluated for metallic particulate contamination before installation of electronic equipment.

RQS N. 03/2005 - CN
CPMI - CORREIOS
1658
Fls:
3701
Doc:

Electrostatic Discharge (ESD) Prevention

Static charges (voltage levels) occur when objects are separated or rubbed together. The voltage level of a static charge is determined by the following factors:

- Types of materials
- Relative humidity
- Rate of change or separation

Table C-1 Effect of Humidity on ESD Charge Levels

Personnel Activity[a]	Humidity[b] and Charge Levels (voltages)[c]			
	26%	32%	40%	50%
Person walking across a linoleum floor	**6,150 V**	**5,750 V**	**4,625 V**	**3,700 V**
Person walking across a carpeted floor	18,450 V	17,250 V	13,875 V	11,100 V
Person getting up from a plastic chair	24,600 V	23,000 V	18,500 V	14,800 V

a. Source: B.A. Unger, Electrostatic Discharge Failures of Semiconductor Devices (Bell Laboratories, 1981)
b. For the same relative humidity level, a high rate of airflow produces higher static charges than a low airflow rate.
c. Some data in this table has been extrapolated.

Static Protection Measures

Follow these precautions to minimize possible ESD-induced failures in the computer room:

- Maintain recommended humidity level and airflow rates in the computer room.
- Install conductive flooring (conductive adhesive must be used when laying tiles).
- Use conductive wax if waxed floors are necessary.
- Ensure that all equipment and flooring are properly grounded and are at the same ground potential.
- Use conductive tables and chairs.
- Use a grounded wrist strap (or other grounding method) when handling circuit boards.
- Store spare electronic modules in antistatic containers.

Acoustics

Computer equipment and air conditioning blowers cause computer rooms to be noisy. Ambient noise level in a computer room can be reduced as follows:

- Dropped ceiling—Cover with a commercial grade of fire-resistant, acoustic rated, fiberglass ceiling tile.
- Sound deadening—Cover the walls with curtains or other sound deadening material.
- Removable partitions—Use foam rubber models for most effectiveness.

ECT
1/4.718
J
CPL - AC

Facility Characteristics

This section contains information about facility characteristics that must be considered for the installation or operation of an hp server. Facility characteristics are:

- Floor loading
- Windows
- Altitude effects

Floor Loading

The computer room floor must be able to support the total weight of the installed hp server as well as the weight of the individual cabinets as they are moved into position.

Floor loading is usually not an issue in nonraised floor installations. The information presented in this section is directed toward raised floor installations.

NOTE An appropriate floor system consultant should verify any floor system under consideration for an hp server installation.

Raised Floor Loading

Raised floor loading is a function of the manufacturer's load specification and the positioning of the equipment relative to the raised floor grid. While Hewlett-Packard cannot assume responsibility for determining the suitability of a particular raised floor system, it does provide information and illustrations for the customer or local agencies to determine installation requirements.

The following guidelines are recommended:

- Because many raised floor systems do not have grid stringers between floor stands, the lateral support for the floor stands depends on adjacent panels being in place. To avoid compromising this type of floor system while gaining under floor access, remove only one floor panel at a time.
- Larger floor grids (bigger panels) are generally rated for lighter loads.

CAUTION Do not position or install any equipment cabinets on the raised floor system until you have carefully examined it to verify that it is adequate to support the appropriate installation.

Floor Loading Terms

Table C-2 Floor Loading Term Definitions

Term	Definition
Dead load	The weight of the raised panel floor system, including the understructure. Expressed in lb/ft2 (kg/m2).
Live load	The load that the floor system can safely support. Expressed in lb/ft2 (kg/m2).

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1659
Fls:
Doc. 3701

Table C-2 Floor Loading Term Definitions (Continued)

Term	Definition
Concentrated load	The load that a floor panel can support on a 1-in2 (6.45 cm2) area at the panel's weakest point (typically the center of the panel), without the surface of the panel deflecting more than a predetermined amount.
Ultimate load	The maximum load (per floor panel) that the floor system can support without failure. Failure expressed by floor panel(s) breaking or bending. Ultimate load is usually stated as load per floor panel.
Rolling load	The load a floor panel can support (without failure) when a wheel of specified diameter and width is rolled across the panel.
Average floor load	Computed by dividing total equipment weight by the area of its footprint. This value is expressed in lb/ft2 (kg/m2).

Average Floor Loading

The average floor load value is not appropriate for addressing raised floor ratings at the floor grid spacing level. However, it is useful for determining floor loading at the building level, such as the area of solid floor or span of raised floor tiles covered by the hp server footprint.

Typical Raised Floor Site

This section contains an example of a computer room raised floor system that is satisfactory for the installation of an hp server.

Based on specific information provided by Hewlett-Packard, Tate Access Floors has approved its Series 800 all-steel access floor with bolt-together stringers and 24 in. (61.0 cm) by 24 in. (61.0 cm) floor panels.

In the event that the flooring is being replaced or a new floor is being installed, Tate Access Floors recommends its Series 1250 all-steel access floor with bolt-together stringers and 24 in. (61.0 cm) by 24 in. (61.0 cm) floor panels be used to support the hp installation.

NOTE If the specific floor being evaluated or considered is other than a Tate Series 800 floor, the specific floor manufacturer must be contacted to evaluate the floor being used.

The following table lists specifications for the Tate Access Floors Series 800 raised floor system.

Table C-3 Typical Raised Floor Specifications

Item[a]	Rating
Dead load	7 lb/ft 2 (34.2 kg/m2)
Live load	313 lb/ft 2 (1528.3 kg/m2)
Concentrated load[b]	1250 lb (567 kg)

E.C.T.
4.718
1
AC

Table C-3 Typical Raised Floor Specifications (Continued)

Item[a]	Rating
Ultimate load	4000 lb (1814 kg) per panel
Rolling load	400 lb (181 kg)
Average floor load	500 lb (227 kg)

a. From Table C-2 on page 203
b. With 0.08 in (0.2 cm) of span maximum deflection

Windows

Avoid housing computers in a room with windows. Sunlight entering a computer room may cause problems. Magnetic tape storage media is damaged if exposed to direct sunlight. Also, the heat generated by sunlight places an additional load on the cooling system.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1660
Fls:
Doc: 3701

Space Requirements

This section contains information about space requirements for an hp server. This data should be used as the basic guideline for space plan developments. Other factors, such as airflow, lighting, and equipment space requirements must also be considered.

Delivery Space Requirements

There should be enough clearance to move equipment safely from the receiving area to the computer room. Permanent obstructions, such as pillars or narrow doorways, can cause equipment damage.

Delivery plans should include the possible removal of walls or doors.

Operational Space Requirements

Other factors must be considered along with the basic equipment dimensions. Reduced airflow around equipment causes overheating, which can lead to equipment failure. Therefore, the location and orientation of air conditioning ducts, as well as airflow direction, are important. Obstructions to equipment intake or exhaust airflow must be eliminated.

The locations of lighting fixtures and utility outlets affect servicing operations. Plan equipment layout to take advantage of lighting and utility outlets. Do not forget to include clearance for opening and closing equipment doors.

Clearance around the cabinets must be provided for proper cooling airflow through the equipment.

If other equipment is located so that it exhausts heated air near the cooling air intakes of the hp server cabinets, larger space requirements are needed to keep ambient air intake to the hp server cabinets within the specified temperature and humidity ranges.

Space planning should also include the possible addition of equipment or other changes in space requirements. Equipment layout plans should also include provisions for the following:

- Channels or fixtures used for routing data cables and power cables
- Access to air conditioning ducts, filters, lighting, and electrical power hardware
- Power conditioning equipment
- Cabinets for cleaning materials
- Maintenance area and spare parts

Floor Plan Grid

A floor plan grid is used to plan the location of equipment in the computer room. In addition to its use for planning, the floor plan grid should also be used when planning the locations of the following items:

- Air conditioning vents
- Lighting fixtures
- Utility outlets
- Doors
- Access areas for power wiring, air conditioning filters and equipment cable routing.

4.734

Typical Installation Schedule

The following schedule lists the sequence of events for a typical system installation:

- 60 days before installation
  - — Floor plan design completed and mailed to Hewlett-Packard (if required to be an HP task)
- 30 days before installation
  - — Primary power and air conditioning installation completed
  - — Telephone and data cables installed
  - — Fire protection equipment installed
  - — Major facility changes completed
  - — Special delivery requirements defined
  - — Site inspection survey completed
  - — Delivery survey completed
  - — A signed copy of the site inspection and delivery survey mailed to Hewlett-Packard
  - — Site inspection and predelivery coordination meeting arranged with a Hewlett-Packard representative to review the inspection checklist and arrange an installation schedule.
- 7 days before installation
  - — Final check made with an Hewlett-Packard site preparation specialist to resolve any last minute problems

NOTE Not all installations follow a schedule like the one noted above. Sometimes, an hp server is purchased through another vendor which can preclude a rigid schedule. Other conditions could also prevent following this schedule. For those situations, consider a milestone schedule.

- Site Preparation - schedule with the customer as soon as possible after the order is placed.
- Site Verification - schedule with the customer a minimum of one to two days before the hp server is scheduled to be installed.

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1661
Doc: 370

Site Inspection

Table C-4 Customer and Hewlett-Packard Information

Customer Information	
Name:	Phone No:
Street Address:	City or Town:
State or Province:	Country
Zip or postal code:	
Primary customer contact:	Phone No.:
Secondary customer contact:	Phone No.:
Traffic coordinator:	Phone No.:
Hewlett-Packard information	
Sales representative	Order No:
Representative making survey	Date:
Scheduled delivery date	

E C T
4.712 1
J
C O L . AC

Table C-5 Site Inspection Checklist

Please check either Yes or No. If No, include comment# or date				Comment or Date
Computer room				
No.	Area or condition	Yes	No	
1.	Is there a completed floor plan?			
2.	Is there adequate space for maintenance needs? Front 36 in (91.4 cm) minimum, Rear 36 in (91.4 cm) minimum are recommended clearances?			
3.	Is access to the site or computer room restricted?			
4.	Is the computer room structurally complete? Expected date of completion?			
5.	Is a raised floor installed and in good condition?			
6.	Is the raised floor adequate for equipment loading?			
7.	Are there channels or cutouts for cable routing?			
8.	Is there a remote console telephone line available with an RJ11 jack?			
9.	Is a telephone line available?			
10.	Are customer supplied peripheral cables and LAN cables available and of the proper type?			
11.	Are floor tiles in good condition and properly braced?			
12.	Is floor tile underside shiny or painted? If painted, judge the need for particulate test.			
Power and lighting				
No.	Area or condition	Yes	No	
13.	Are lighting levels adequate for maintenance?			
14.	Are there AC outlets available for servicing needs? (i.e. vacuuming)			
15.	Does the input voltage correspond to equipment specifications?			
15A	Is dual source power used? If so, identify type(s) and evaluate grounding.			

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1662
Fls:
Doc: 3701

Table C-5 Site Inspection Checklist (Continued)

Please check either Yes or No. If No, include comment# or date				Comment or Date
16	Does the input frequency correspond to equipment specifications?			
17.	Are lightning arrestors installed inside the building?			
18.	Is power conditioning equipment installed?			
19.	Is there a dedicated branch circuit for equipment?			
20.	Is the dedicated branch circuit less than 250 feet (72.5 meters)?			
21.	Are the input circuit breakers adequate for equipment loads?			
Safety				
No.	Area or condition	Yes	No	
22.	Is there an emergency power shut-off switch?			
23.	Is there a telephone available for emergency purposes?			
24.	Is there a fire protection system in the computer room?			
25.	Is antistatic flooring installed?			
26.	Are there any equipment servicing hazards (loose ground wires, poor lighting, etc.)?			
Cooling				
No.	Area or condition	Yes	No	
27.	Can cooling be maintained between 20 °C and 55 °C (up to 5000 ft.)? Derate 1 °C/1000 ft. above 5000 ft. and up to 10,000 ft.			
28.	Can temperature changes be held to 10 °C per hour with tape media? Can temperature changes be held to 20 °C per hour without tape media?			
29.	Can humidity level be maintained at 40% to 60% at 35 °C noncondensing?			
30.	Are air conditioning filters installed and clean?			
Storage				

ECT
CPL - AC.

Table C-5 Site Inspection Checklist (Continued)

Please check either Yes or No. If No, include comment# or date				Comment or Date
No.	Area or condition	Yes	No	
31.	Are cabinets available for tape and disc media?			
32.	Is shelving available for documentation?			
Training				
No.	Area or Condition			
33	Are personnel enrolled in the System Administrator's Course?			
34	Is on-site training required?			

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1663
Fls: 370
Doc:

Delivery Survey

The delivery survey forms list delivery or installation requirements. If any of the items on the list apply, enter the appropriate information in the areas provided on the form.

Special instructions or recommendations should be entered on the special instructions or recommendations form. The following list gives examples of special instructions or issues:

- Packaging restrictions at the facility, such as size and weight limitations
- Special delivery procedures
- Special equipment required for installation, such as tracking or hoists
- What time the facility is available for installation (after the equipment is unloaded)
- Special security requirements applicable to the facility, such as security clearance

E C T
4.708
L
CPL - AC

Figure C-2 Delivery Survey (Part 1)

DELIVERY CHECKLIST

DOCK DELIVERY

Is dock large enough for a semitrailer? Yes _____ No _____

Circle the location of the dock and give street name if different than address.

North

West East

South

STREET DELIVERY

Circle the location of access door and list street name if different than address.

North

West East

South

List height _____ and width _____ of access door.

List special permits (if required) for street delivery.

Permit type: Agency obtained from:

_____ _____

_____ _____

60SP018A
12/7/99

RQS Nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1664
Doc: 3701

Figure C-3 Delivery Survey (Part 2)

ELEVATOR

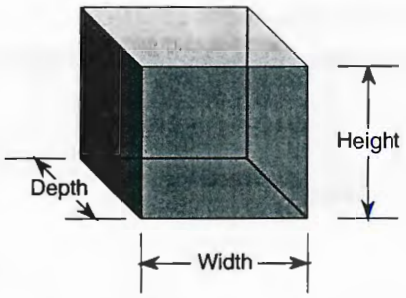
Fill in the following information if an elevator is required to move equipment.

Capacity (lb or kg) _____

Depth _____

Height _____

Width _____



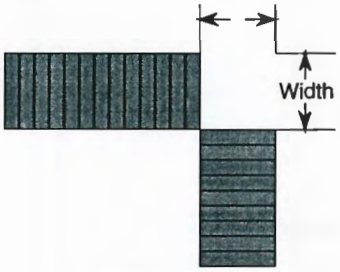
STAIRS

Please list number of flights and stairway dimensions.

Number of flights _____

Width _____

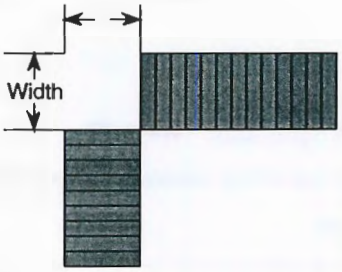
Width _____



Number of flights _____

Width _____

Width _____



60SP019A
11/24/99

A

Accessing Error Chassis Logs, 98
Acoustic Safety Standards, 248
Adding Users, 71, 80, 83
Additional Components, 22
Altitude Operation Standards, 249
  Effects of Altitude, 249

C

Cabinet Performance Grounding (High Frequency Ground), 255
Changing the Default GSP Configuration, 82, 85
Chassis Code to FRU Decode, 93
Computer Room Physical Space Requirements, 243
  Aisle Space, 243
  Server, 243
Computer Room Unpacking Space, 244
Configure Remote Console, 60
Configure RS-232 Console, 56
Configure System Consoles, 55
Configure the LAN Console, 61
Configure the Web Console, 63
Configuring the GSP LAN Port, 80, 83
Configuring the GSP LAN Port via an ASCII console, 61
Configuring the Rev A Guardian Service Processor (GSP), 80
Configuring the Rev B Guardian Service Processor (GSP), 83
Core I/O Connections, 50
Core I/O Removal, 146
Core I/O Replacement, 147
CPU Removal, 182
CPU Socket Replacement, Cleaning, and CPU Replacement, 183
  Cleaning Kit Components, 183
  CPU Cleaning for System Board Replacement, 185, 186
  Replacing the CPU, 187
  Tools Required, 183
Cross-Referencing Chassis Log Errors to rp54xx FRUs, 93
CRU Physical Location, 216
Customer Replaceable Unit Part Numbers, 219

D

Data Communications Cables, 257
Determine Current System State, 88
Dimensions, 242
Disk Media Backplane Removal, 212
Disk Media Backplane Replacement, 213
Disk Media Housing Removal, 188
Disk Media Housing Replacement, 189
Display Board Removal, 173, 174
  Removing rp5400 and/or rp5450 Model Platform Monitors, 175
  Removing The rp5470 Model Platform Monitor, 175

E

Electrical, 245
  Modular PDUs, 246
  Office High Availability Requirements, 245
  Server-level Enhanced Power Availability, 245
  Power Protection, 245
  System Power Requirements, 246
electrical and environmental guidelines
  electrical conduit ground, 255
  electrostatic discharge prevention, 248
  lighting requirements, 252
  main building electrical ground, 255
  power panel grounds, 255
Electrical Conduit Ground, 255
electrical load requirements, 253
Environment Elements
  Acoustics, 262
Environmental Elements, 258
  Computer Room Preparation, 258
  Cooling Requirements, 258
    Air Conditioning Ducts, 260
    Air Conditioning System Guidelines, 259
    Air Conditioning System Installation, 260
    Air Conditioning System Types, 259
    Basic Air Conditioning Equipment Requirements, 258
    Basic Air Distribution Systems, 259
  Delivery Survey, 272
  Dust and Pollution Control, 260
  Electrostatic Discharge (ESD) Prevention, 262
  Facility Characteristics, 263
    Floor Loading, 263
    Average Floor Loading, 264
    Floor Loading Terms, 263
    Raised Floor Loading, 263
    Typical Raised Floor Site, 264
    Windows, 265
  Humidity Level, 260
  Metallic Particulate Contamination, 261
  Site Inspection, 268
  Space Requirements, 266
    Delivery Space Requirements, 266
    Floor Plan Grid, 266
    Operational Space Requirements, 266
  Typical Installation Schedule, 267
Equipment Grounding Implementation Details, 257
Example of Accessing Error Logs, 98
Expansion I/O LED States, 116
Extend the Server out the Front, 133

F

Factory Integrated Cabinet Installation, 2
Fan, Power Supply, and Disk LED States, 121
Field Replaceable Unit Part Numbers, 235
Front Bezel Removal (Single Piece), 142
Front Bezel Removal (Two Piece), 144
Front Bezel Replacement (Single Piece), 143
Front Bezel Replacement (Two Piece), 145
FRU Physical Location, 221

G

Graphics Troubleshooting, 46
grounding systems

4.706 L
3701
1665

Index

electrical conduit ground, 255
GSP Cables, 56
GSP Configurable Parameters, 71
GSP Features, 53
GSP LAN, 53
GSP LED States, 118
GSP RS-232, 53
Guardian Service Processor (GSP) Overview, 53

H

hot swap procedure
  software, 151
HotPlug
  Hardware HotPlug Procedure, 156
  Hot Swap Procedure for Unattached Physical Volumes, 158
  Hot Swap Software Procedure for Attached Physical Volumes, 157
HotPlug Disk Drive Removal, 151
HotPlug Disk Drive Replacement, 156
HotSwap Card Cage Fan Removal, 163
HotSwap Card Cage Fan Replacement, 164
HotSwap Chassis Fan Cover Removal, 159
HotSwap Chassis Fan Cover Replacement, 160
HotSwap Chassis Fan Removal, 161
HotSwap Chassis Fan Replacement, 162
HotSwap Power Converter Fan Removal, 167
HotSwap Power Converter Fan Replacement, 168
HotSwap Power Supply Removal, 165
HotSwap Power Supply Replacement, 166

I

Identifying Approved Non-E-Series HP Cabinets, 17
Identifying E-Series HP Cabinets, 18
Identifying Static Rail Kit, 18
Individual Component Remove/Replace Instructions, 133
Initial Power-up, 76
Insert the Server from the Front, 134
Install Deskside server, 8
Install Stand-Alone Server in a Cabinet, 11
Installing a PCI Card, 36
Installing Central Processing Units (CPUs), 23
Installing Disk Drives, 47
Installing Graphics, 39
Installing Memory, 28
Installing Peripheral Component Interconnect (PCI) Cards, 32
Installing rp5400 and/or rp5450 DIMMs, 28
Installing rp5470 DIMMs, 30
Installing Stationary Rails, 19
Interpreting Chassis Logs Using the chassis_code.codes File, 100
Interpreting Service Processor Error Chassis Logs, 98
Interpreting System Alerts, 96, 97

K

Key FRU Identification Fields for Error Chassis Logs, 99
Key FRU Identification Fields for System Alerts, 97

L

Power Distribution Safety Grounding, 255
Site Preparation
  Distribution Hardware
    Raceway Systems (electrical conduits), 254
LAN and Telephone, 247
LAN/SCSI LED States, 120
lighting requirements, 253

M

Memory Configuration Rules, 28
Memory DIMM Removal, 171

  Removing rp5400 Memory DIMMs, 171
  Removing rp5470 Memory DIMMs, 171
Memory DIMM Replacement, 172
  Replacing rp5400 and/or rp5450 Memory DIMMs, 172
  Replacing rp5470 Memory DIMMs, 172

O

Online Addition/Replacement (OLA/R) of PCI I/O cards, 38

P

PCI Backplane Removal, 206
  Removing rp5400 and/or rp5450 PCI Backplanes, 206
  Removing rp5470 PCI Backplane, 207
PCI Backplane Replacement, 209
  Replacing rp5400 and/or rp5450 PCI Backplanes, 209
  Replacing rp5470 PCI Backplane, 211
PCI Card Separator/Extractor Removal, 149
PCI Card Separator/Extractor Replacement, 150
PCI I/O Card Installation Order, 34
PCI I/O Card Installation Restrictions, 34
PCI I/O Card Removal, 179
PCI I/O Card Replacement, 180
PCI I/O LED States, 114
Platform Monitor Replacement, 177
  Replacing rp5400 and/or rp5450 Platform Monitors, 177
  Replacing rp5470 Platform Monitor, 177
Power Converter Removal, 193
Power Converter Replacement, 194
Power Panel Ground, 255
Power Supply Failure Example, 95
Problem Symptoms and Repair Actions, 89
Processor Failure Example, 95
Processor Support Module Removal, 169
Processor Support Module Replacement, 170

R

raised floor
  ground system, illustrated, 256
Raised Floor "High Frequency Noise" Grounding, 256
Receive/Unpack A Non-Integrated Server, 5
Removable Media Removal, 190
Removable Media Replacement, 191

E C T
4.7121
J
C O L - AC

Table C-5 Site Inspection Checklist

Please check either Yes or No. If No, include comment# or date				Comment or Date
Computer room				
No.	Area or condition	Yes	No	
1.	Is there a completed floor plan?			
2.	Is there adequate space for maintenance needs? Front 36 in (91.4 cm) minimum, Rear 36 in (91.4 cm) minimum are recommended clearances.			
3.	Is access to the site or computer room restricted?			
4.	Is the computer room structurally complete? Expected date of completion?			
5.	Is a raised floor installed and in good condition?			
6.	Is the raised floor adequate for equipment loading?			
7.	Are there channels or cutouts for cable routing?			
8.	Is there a remote console telephone line available with an RJ11 jack?			
9.	Is a telephone line available?			
10.	Are customer supplied peripheral cables and LAN cables available and of the proper type?			
11.	Are floor tiles in good condition and properly braced?			
12.	Is floor tile underside shiny or painted? If painted, judge the need for particulate test.			
Power and lighting				
No.	Area or condition	Yes	No	
13.	Are lighting levels adequate for maintenance?			
14.	Are there AC outlets available for servicing needs? (i.e. vacuuming)			
15.	Does the input voltage correspond to equipment specifications?			
15A	Is dual source power used? If so, identify type(s) and evaluate grounding.			

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1666
Fls:
3701
Doc:

Table C-5 Site Inspection Checklist (Continued)

Please check either Yes or No. If No, include comment# or date				Comment or Date
16	Does the input frequency correspond to equipment specifications?			
17.	Are lightning arrestors installed inside the building?			
18.	Is power conditioning equipment installed?			
19.	Is there a dedicated branch circuit for equipment?			
20.	Is the dedicated branch circuit less than 250 feet (72.5 meters)?			
21.	Are the input circuit breakers adequate for equipment loads?			
Safety				
No.	Area or condition	Yes	No	
22.	Is there an emergency power shut-off switch?			
23.	Is there a telephone available for emergency purposes?			
24.	Is there a fire protection system in the computer room?			
25.	Is antistatic flooring installed?			
26.	Are there any equipment servicing hazards (loose ground wires, poor lighting, etc.)?			
Cooling				
No.	Area or condition	Yes	No	
27.	Can cooling be maintained between 20 °C and 55 °C (up to 5000 ft.)? Derate 1 °C/1000 ft. above 5000 ft. and up to 10,000 ft.			
28.	Can temperature changes be held to 10 °C per hour with tape media? Can temperature changes be held to 20 °C per hour without tape media?			
29.	Can humidity level be maintained at 40% to 60% at 35 °C noncondensing?			
30.	Are air conditioning filters installed and clean?			
Storage				

E C T
CPL - AC

Table C-5 Site Inspection Checklist (Continued)

Please check either Yes or No. If No, include comment# or date				Comment or Date
No.	Area or condition	Yes	No	
31.	Are cabinets available for tape and disc media?			
32.	Is shelving available for documentation?			
Training				
No.	Area or Condition			
33	Are personnel enrolled in the System Administrator's Course?			
34	Is on-site training required?			

RQS Nº 03/2005 - C
CPMI - CORREIOS
1667
Fls:
3701
Doc:

Delivery Survey

The delivery survey forms list delivery or installation requirements. If any of the items on the list apply, enter the appropriate information in the areas provided on the form.

Special instructions or recommendations should be entered on the special instructions or recommendations form. The following list gives examples of special instructions or issues:

- Packaging restrictions at the facility, such as size and weight limitations
- Special delivery procedures
- Special equipment required for installation, such as tracking or hoists
- What time the facility is available for installation (after the equipment is unloaded)
- Special security requirements applicable to the facility, such as security clearance

E C T
4.708
L
CPL - AC

Figure C-2 Delivery Survey (Part 1)

DELIVERY CHECKLIST

DOCK DELIVERY

Is dock large enough for a semitrailer? Yes _____ No _____

Circle the location of the dock and give street name if different than address.

North

West East

South

STREET DELIVERY

Circle the location of access door and list street name if different than address.

North

West East

South

List height _____ and width _____ of access door.

List special permits (if required) for street delivery.

Permit type: Agency obtained from:

_____ _____

_____ _____

60SP018A
12/7/99

RQS Nº 03/2005 - CN
CPMI - CORREIOS
1668
Fls:
Doc: 3713

Figure C-3 Delivery Survey (Part 2)

ELEVATOR

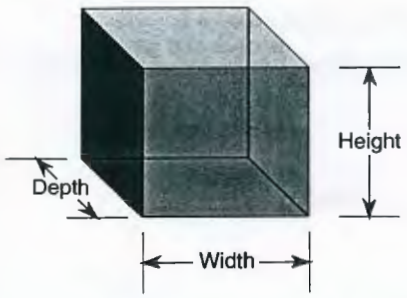
Fill in the following information if an elevator is required to move equipment.

Capacity (lb or kg) _____

Depth _____

Height _____

Width _____



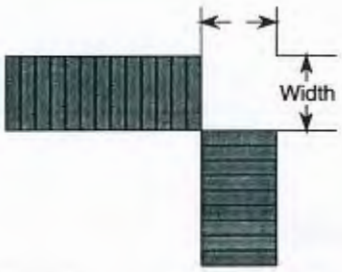
STAIRS

Please list number of flights and stairway dimensions.

Number of flights _____

Width _____

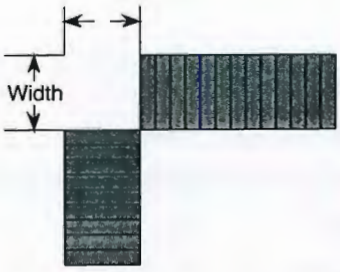
Width _____



Number of flights _____

Width _____

Width _____



60SP019A
11/24/99

A

Accessing Error Chassis Logs, 98
Acoustic Safety Standards, 248
Adding Users, 71, 80, 83
Additional Components, 22
Altitude Operation Standards, 249
  Effects of Altitude, 249

C

Cabinet Performance Grounding (High Frequency Ground), 255
Changing the Default GSP Configuration, 82, 85
Chassis Code to FRU Decode, 93
Computer Room Physical Space Requirements, 243
  Aisle Space, 243
  Server, 243
Computer Room Unpacking Space, 244
Configure Remote Console, 60
Configure RS-232 Console, 56
Configure System Consoles, 55
Configure the LAN Console, 61
Configure the Web Console, 63
Configuring the GSP LAN Port, 80, 83
Configuring the GSP LAN Port via an ASCII console, 61
Configuring the Rev A Guardian Service Processor (GSP), 80
Configuring the Rev B Guardian Service Processor (GSP), 83
Core I/O Connections, 50
Core I/O Removal, 146
Core I/O Replacement, 147
CPU Removal, 182
CPU Socket Replacement, Cleaning, and CPU Replacement, 183
  Cleaning Kit Components, 183
  CPU Cleaning for System Board Replacement, 185, 186
  Replacing the CPU, 187
  Tools Required, 183
Cross-Referencing Chassis Log Errors to rp54xx FRUs, 93
CRU Physical Location, 216
Customer Replaceable Unit Part Numbers, 219

D

Data Communications Cables, 257
Determine Current System State, 88
Dimensions, 242
Disk Media Backplane Removal, 212
Disk Media Backplane Replacement, 213
Disk Media Housing Removal, 188
Disk Media Housing Replacement, 189
Display Board Removal, 173, 174
  Removing rp5400 and/or rp5450 Model Platform Monitors, 175
  Removing The rp5470 Model Platform Monitor, 175

E

Electrical, 245
  Modular PDUs, 246
  Office High Availability Requirements, 245
  Server-level Enhanced Power Availability, 245
  Power Protection, 245
  System Power Requirements, 246
electrical and environmental guidelines
  electrical conduit ground, 255
  electrostatic discharge prevention, 248
  lighting requirements, 252
  main building electrical ground, 255
  power panel grounds, 255
Electrical Conduit Ground, 255
electrical load requirements, 253
Environment Elements
  Acoustics, 262
Environmental Elements, 258
  Computer Room Preparation, 258
  Cooling Requirements, 258
    Air Conditioning Ducts, 260
    Air Conditioning System Guidelines, 259
    Air Conditioning System Installation, 260
    Air Conditioning System Types, 259
    Basic Air Conditioning Equipment Requirements, 258
  Basic Air Distribution Systems, 259
  Delivery Survey, 272
  Dust and Pollution Control, 260
  Electrostatic Discharge (ESD) Prevention, 262
  Facility Characteristics, 263
    Floor Loading, 263
    Average Floor Loading, 264
    Floor Loading Terms, 263
    Raised Floor Loading, 263
    Typical Raised Floor Site, 264
    Windows, 265
  Humidity Level, 260
  Metallic Particulate Contamination, 261
  Site Inspection, 268
  Space Requirements, 266
    Delivery Space Requirements, 266
    Floor Plan Grid, 266
    Operational Space Requirements, 266
  Typical Installation Schedule, 267
Equipment Grounding Implementation Details, 257
Example of Accessing Error Logs, 98
Expansion I/O LED States, 116
Extend the Server out the Front, 133

F

Factory Integrated Cabinet Installation, 2
Fan, Power Supply, and Disk LED States, 121
Field Replaceable Unit Part Numbers, 235
Front Bezel Removal (Single Piece), 142
Front Bezel Removal (Two Piece), 144
Front Bezel Replacement (Single Piece), 145
Front Bezel Replacement (Two Piece), 145
FRU Physical Location, 221

G

Graphics Troubleshooting, 46
grounding systems

ECT 1 / 4.706 / L / L - AC

BOS Nº 03/2005 - ON
CPMI - CORREIOS
1669
Fls:
Doc: 3701

Index

electrical conduit ground, 255
GSP Cables, 56
GSP Configurable Parameters, 71
GSP Features, 53
GSP LAN, 53
GSP LED States, 118
GSP RS-232, 53
Guardian Service Processor (GSP) Overview, 53

H

hot swap procedure
  software, 151
HotPlug
  Hardware HotPlug Procedure, 156
  Hot Swap Procedure for Unattached Physical Volumes, 158
  Hot Swap Software Procedure for Attached Physical Volumes, 157
HotPlug Disk Drive Removal, 151
HotPlug Disk Drive Replacement, 156
HotSwap Card Cage Fan Removal, 163
HotSwap Card Cage Fan Replacement, 164
HotSwap Chassis Fan Cover Removal, 159
HotSwap Chassis Fan Cover Replacement, 160
HotSwap Chassis Fan Removal, 161
HotSwap Chassis Fan Replacement, 162
HotSwap Power Converter Fan Removal, 167
HotSwap Power Converter Fan Replacement, 168
HotSwap Power Supply Removal, 165
HotSwap Power Supply Replacement, 166

I

Identifying Approved Non-E-Series HP Cabinets, 17
Identifying E-Series HP Cabinets, 18
Identifying Static Rail Kit, 18
Individual Component Remove/Replace Instructions, 133
Initial Power-up, 76
Insert the Server from the Front, 134
Install Deskside server, 8
Install Stand-Alone Server in a Cabinet, 11
Installing a PCI Card, 36
Installing Central Processing Units (CPUs), 23
Installing Disk Drives, 47
Installing Graphics, 39
Installing Memory, 28
Installing Peripheral Component Interconnect (PCI) Cards, 32
Installing rp5400 and/or rp5450 DIMMs, 28
Installing rp5470 DIMMs, 30
Installing Stationary Rails, 19
Interpreting Chassis Logs Using the chassis_code.codes File, 100
Interpreting Service Processor Error Chassis Logs, 98
Interpreting System Alerts, 96, 97

K

Key FRU Identification Fields for Error Chassis Logs, 99
Key FRU Identification Fields for System Alerts, 97

L

Power Distribution Safety Grounding, 255
Site Preparation
  Distribution Hardware
    Raceway Systems (electrical conduits), 254
LAN and Telephone, 247
LAN/SCSI LED States, 120
lighting requirements, 253

M

Memory Configuration Rules, 28
Memory DIMM Removal, 171

  Removing rp5400 Memory DIMMs, 171
  Removing rp5470 Memory DIMMs, 171
Memory DIMM Replacement, 172
  Replacing rp5400 and/or rp5450 Memory DIMMs, 172
  Replacing rp5470 Memory DIMMs, 172

O

Online Addition/Replacement (OLA/R) of PCI I/O cards, 38

P

PCI Backplane Removal, 206
  Removing rp5400 and/or rp5450 PCI Backplanes, 206
  Removing rp5470 PCI Backplane, 207
PCI Backplane Replacement, 209
  Replacing rp5400 and/or rp5450 PCI Backplanes, 209
  Replacing rp5470 PCI Backplane, 211
PCI Card Separator/Extractor Removal, 149
PCI Card Separator/Extractor Replacement, 150
PCI I/O Card Installation Order, 34
PCI I/O Card Installation Restrictions, 34
PCI I/O Card Removal, 179
PCI I/O Card Replacement, 180
PCI I/O LED States, 114
Platform Monitor Replacement, 177
  Replacing rp5400 and/or rp5450 Platform Monitors, 177
  Replacing rp5470 Platform Monitor, 177
Power Converter Removal, 193
Power Converter Replacement, 194
Power Panel Ground, 255
Power Supply Failure Example, 95
Problem Symptoms and Repair Actions, 89
Processor Failure Example, 95
Processor Support Module Removal, 169
Processor Support Module Replacement, 170

R

raised floor
  ground system, illustrated, 256
Raised Floor "High Frequency Noise" Grounding, 256
Receive/Unpack A Non-Integrated Server, 5
Removable Media Removal, 190
Removable Media Replacement, 191

SCSI ID Settings, 191
Remove and Replace Procedures by Part, 124
Removing Users, 72, 82, 85
Return the GSP to Default Configurations, 73
Revision A GSP, 50, 54
Revision B GSP, 51, 54
rp5400 and rp5450 I/O Block Diagram, 103
rp5400 and rp5450 System Block Diagram, 102
rp5400/rp5450 PCI Card Slots, 32
rp5430 and rp5470 System Block Diagram, 104, 105
rp5470 PCI Card Slots, 33
rp54xx Server Boot Process, 74
Run/Attention/Fault LED States, 106

S

Sample System Alerts, 97
Secure Web Console Installation, 68
Side Cover Removal, 140
Side Cover Replacement, 141
Site Preparation
  Computer Room Safety, 252
    Fire Protection, 252
    Lighting Requirements for Equipment Servicing, 252
  Distribution Hardware, 254
    Building Distribution, 254
    Wire Selection, 254
  Electrical Factors, 252
  Electrical Load Requirements (Circuit Breaker Sizing), 253
  Grounding Systems, 255
  Power Consumption, 253
  Power Quality, 253
    Power System Protection, 254
    Sources of Voltage Fluctuations, 253
Space Requirements, 242
Stand-alone Server Cover Removal, 135
Stand-alone Server Cover Replacement, 137
Stationary L-Bracket Rail Assembly, 17
System Board Removal, 195
  Removing rp5400 and/or rp5450 Model System Boards, 195
  Removing rp5470 Model System Board, 196
System Board Replacement, 197
  rp5400 or rp5450 System Board Replacement, 197
    Configuring System Board, 198
  rp5470 System Board Replacement, 201
    Power up procedure., 204
System Installation Guidelines, 257

T

Temperature and Humidity Operating Standards, 250
  Thermal Protection Features, 250
Top Cover Removal, 138
Top Cover Replacement, 139
Troubleshooting and FRU identification, 89

U

Uncrating Space, 242
Unpacking the SPU, 5

V

V-Class system
  temperature and humidity specifications, 250

W

Wiring Connections, 257

ECT 1 4-704 1 CPL - AC

TRG Nº 03/2005 - CI
CPMI - CORREIOS
Fls: 1670
Doc: 3701