CPL/AC

PREGÃO
050/2003

LOCAÇÃO DE EQUIPAMENTOS DE INFORMÁTICA INCLUINDO ASSISTÊNCIA TÉCNICA E TREINAMENTO

COBRA TECNOLOGIA – MANUAL VOLUME 12

2003
PASTA 40

COBRA TECNOLOGIA

Integradora de Soluções em TI e Serviços

ANEXO SERVIDOR PARA DETECÇÃO DE INTRUSOS
PARTE 2

COBRA Tecnologia S.A.
Estrada dos Bandeirantes 7966
CEP 22783-110 Rio de Janeiro RJ
Tel: 21 2142-9600
www.cobra.com.br

Cisco Systems

Data Sheet

Management Center for **IDS Sensors**, Version 1.2

Introduction

The Management Center for IDS Sensors is a tool with a scalable architecture for configuring Cisco network sensors, switch IDS sensors, and IDS network modules for routers. With the Management Center for IDS Sensors, administrators can save considerable time by configuring multiple sensors concurrently using group profiles. Additionally, it provides a powerful signature management feature that increases the accuracy and specificity of detecting possible network intrusions.

The Management Center for IDS Sensors is a component of the CiscoWorks VPN/ Security Management Solution (VMS). VMS is an integral part of the SAFE blueprint and combines web-based tools for configuring, monitoring and troubleshooting:

- Virtual Private Networks (VPN)
- Firewalls
- Network Intrusion Detection Systems (IDS)
- Host-based IDS.

CiscoWorks VMS addresses the needs of both small- and large-scale VPN and security deployments by protecting productivity gains and reducing operating costs fororganizations.

Intended Use

Many enterprises have increased the deployment of Cisco network and switch IDS sensors to provide security against network attacks. The Management Center for IDS Sensors helps centrally manage this rising number of sensors, and provides added security in a way that reduces management time and cost of operations.

This tool has significant feature enhancements and is an evolution from the previous CSPM and IDS Director software.

New Features since v1.0

The Management Center for IDS Sensors, version 1.2 has additional support for IDS 4.0 and 4.1 sensor code. The administrator will see a number of usability enhancements. For example, signatures are now listed by logical groups to help you find signatures much more easily. The operator can enable or disable entire signature groups to customize for a specific networking environment. This can be done with a few clicks, which saves time. Tuning signatures has also become easier enabling more specificity in setting signature parameters.

The Management Center for IDS Sensors, version 1.1 is now supported on Solaris 8. This software does not have some of the

features that are available on the Management Center for IDS Sensors, version 1.2, which is available only on Windows 2000 currently. Examples of features not supported on the Solaris platform include:

- No support for managing Cisco IDS Network Modules for routers
- No support for managing Cisco network IDS and switch IDS sensors that use IDS 4.1

Features and Benefits

Easy to use —Can be utilized without in-depth security expertise:

- Easy to use web-based interface
- "Wizards" to walk the user through common management tasks
- Access to the Network Security Database (NSDB). This will help those without IDS security expertise, by providing meaningful information on alarms.

Centralized management:

- Define hierarchy of sensors, containing groups and subgroups.

Scalability:

- Support several hundred sensor deployments from each console
- Use of a robust relational database to store a high volume of data

Security:

- Five authorization roles to delegate responsibility to different administrators

Workflow model:

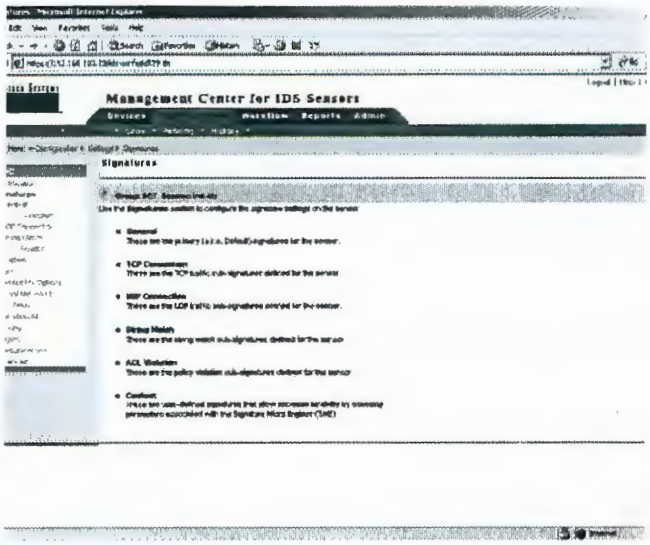
- Determine which administrators can generate, approve and deploy configurations. Separate tasks into a workflow. For example propose changes to an "Approver" before deployment.

Enhanced signature management:

- Create and customize signatures for further tuning

Figure 1

Flexible options to create and tune signatures, to rapidly respond to new threats



Block Attacks:

- Configure a sensor to block an attack by generating ACL rules for a Cisco router or firewall.

Platforms Supported for Configuration	Software Version Supported
Cisco Network IDS sensors	IDS 3.0, 3.1, 4.0, and 4.1
Cisco Switch IDS (IDSM) sensors	IDSM 3.0(5), 4.0, and 4.1
Cisco IDS network module for routers	IDS 4.1

System Requirements

For comprehensive hardware and operating requirements see the VMS Overview at: http://www.cisco.com/go/vms

Ordering Information

The Management Center for IDS Sensors is a featured component of CiscoWorks VMS. For ordering details refer to the VMS Product Bulletin found at:
http://www.cisco.com/go/vms

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

202970/ETMG 9/02

For More Information

Please refer to http://www.cisco.com/go/vms or email ciscoworks@cisco.com.

CISCO SYSTEMS

Data Sheet

Monitoring Center for **Security**, Version 1.2

Introduction

The Monitoring Center for Security is a tool to capture, store, view, correlate and report on events from:

- Cisco Network IDS
- Cisco Switch IDS
- Cisco IDS Network Module for routers
- Management Center for Cisco Security Agents
- Cisco PIX Firewalls
- Cisco Firewall Services Modules
- Cisco IOS Routers

The Monitoring Center for Security will increase the accuracy of threat detection and lower the operational costs for event monitoring, and will increase your administrator's productivity. The software delivers event correlation to identify attacks that are not easily recognizable from a single event, a flexible notification scheme and automated responses to critical events. By taking advantage of user-defined event correlation rules, the operator can:

- Monitor attacks against specific, high visibility hosts (for example, a web server).
- Monitor the traffic for patterns of attacks
- Correlate IDS information from multiple security devices (e.g., firewalls, network IDS, host IDS)
- Receive early notification of emerging threats
- Trigger an automated response, as a corrective action against an attack
- Reduce the number of false positives

The Monitoring Center for Security is a component of the CiscoWorks VPN/ Security Management Solution (VMS). VMS is an integral part of the SAFE blueprint and combines web-based tools for configuring, monitoring and troubleshooting:

- Virtual Private Networks (VPN)
- Firewalls
- Network Intrusion Detection Systems (IDS)
- Host-based IDS

CiscoWorks VMS addresses the needs of both small- and large-scale VPN and security deployments by protecting productivity gains and reducing operating costs fororganizations.

Intended Use

The Monitoring Center for Security will benefit those organizations experiencing information overload, resulting from:

- Too many security consoles
- Too many security events to monitor
- Difficulty in viewing the big security picture

New Features

The Monitoring Center for Security includes support for additional event types. The operator can now monitor events from the Management Center for Cisco Security Agents, version 4.0 and also monitor events from the Cisco Intrusion Detection System (IDS) software version 4.1. The Management Center for Cisco Security Agents 4.0 will receive events from agents and then forward these events to the Monitoring Center for Security version 1.2. As a result, the Monitoring Center for Security provides a broad, unified view of security messages.

Support for IDS 4.1 allows the operator to monitor network IDS sensors that communicate using the Remote Data Exchange Protocol (RDEP). With the RDEP protocol the operator can subscribe to specific IDS event types and better control which events are received.

Enhancements in the event viewer include performance improvements for event deletions and an addition of a new interface graphing capability. The user can also preserve their preferred column ordering in the event viewer.

Enhancements for reporting include the ability to save generated reports to the database and to a file for more flexible storage options. Furthermore, new summary information has been added to reports to help with analysis. Cisco has added more reports for firewalls and Cisco Security Agents.

Enhancements in the notification system include an increase in the number of active events rules from 5 to 10. Event rules help identify critical events and automate a response so that the operator does not need to monitor a screen over long periods. The operator can also import Cisco IDS Sensor configurations from a remote Management Center for IDS Sensors server to save time.

The Monitoring Center for Security, version 1.1 is now supported on Solaris 8. This software does not have some of the features that are available in the Monitoring Center for Security version 1.2, which is available only on Windows 2000 currently. Examples of features not supported on the Solaris platform include:

- No support for events from the Management Center for Cisco Security Agents, version 4.0
- No support for events from the Cisco IDS Network Module for routers
- No support for events form IDS version 4.1 (however, IDS 4.0 is supported)
- No additional reports for firewall and Cisco Security Agents
- No support for saving the preferences of column ordering in the event viewer

Features and Benefits

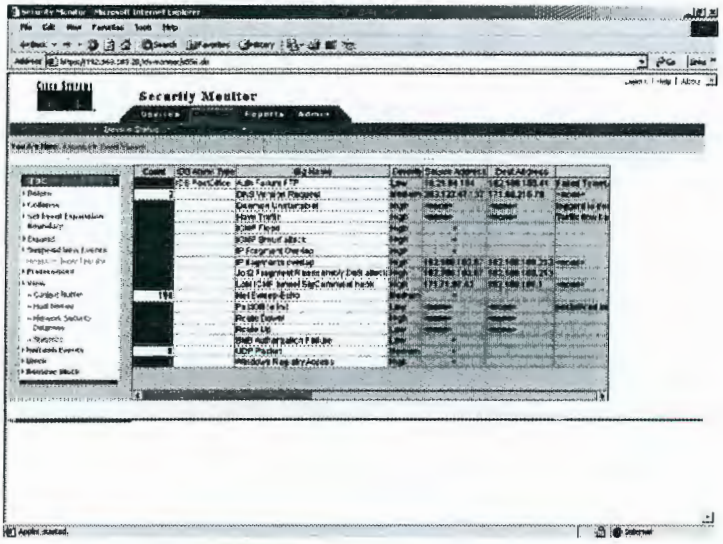
Comprehensive reporting options for finding information

- Web-based wizard for creating flexible security reports
- On-demand and scheduled reports
- Reports by top incidents, by IP address, by time, by signature, by event, etc.
- Send notifications of reports by email

Web-based event viewer with features to easily locate attacks

- Easily "slice and dice" data by moving event field columns and sifting through thousands of events in seconds. The Event Viewer can read both real-time and historical events from the database.

Figure 1
Design based on award winning event viewer.



Perform event correlation to detect an emerging threat

- Create user-defined rules for establishing relationships between events (correlate by type of event, by time, across sensors, across source addresses, etc.). This helps to identify attacks, which may not be apparent from a single event.
- The user can define thresholds and time periods when a rule should be triggered
- If a rule is triggered, the user can be notified via email and fine-tune what information from the suspicious packet is forwarded with the email. Alternatively, the user can automatically execute a script as a corrective response.

Database Management

- The Monitoring Center for Security provides a relational database that is used for storage of event data. Various database management functions such as archiving and purging can easily be performed without database administration skills within the Monitoring Center for Security using the web interface.

Devices Supported for Monitoring

Platform	Software Version Supported
Cisco Network IDS sensors	IDS 3.0, 3.1, 4.0 and 4.1
Cisco Switch IDS (IDSM) sensors	IDSM 3.0(5), 4.0 and 4.1
Cisco IDS Network Module for Cisco Routers	IDS 4.1
Cisco PIX Firewall	Cisco PIX Firewall OS 6.0(x), 6.1(x), 6.2(x), 6.3.1
Cisco Firewall Services Modules	1.1
Cisco IOS Router for IDS messages (with IOS Firewall toolkit)	12.2x mainline and later
Cisco Security Agents (forwarded by Management Center for Cisco Security Agents, version 4.0)	4.0
Cisco IDS Host Console (forwarded by the Cisco IDS Host Console, version 2.5)	2.5

System Requirements

For comprehensive hardware and operating requirements see the VMS Overview.

http://www.cisco.com/go/vms

Ordering Information

The Monitoring Center for Security is a featured component of CiscoWorks VMS. For ordering details click on the VMS Product Bulletin found at:

http://www.cisco.com/go/vms

For More Information

Please reference http://www.cisco.com/go/vms or email ciscoworks@cisco.com

CISCO SYSTEMS

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 317 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

Configuring Sensors and Signatures

Network sensing can be accomplished using either a sensor or an IDSM (Intrusion Detection System Module). Both of these sensing platforms are components of the Cisco Intrusion Detection System and can be managed by IDS MC. Both sensing platforms monitor and analyze network traffic in real time. They do this by looking for anomalies and misuse on the basis of an extensive embedded signature library. However, the two platforms differ in how they can respond to perceived intrusions.

The sensor is a high-performance plug-and-play appliance. When it detects unauthorized network activity, the sensor can terminate the connection, permanently block the associated host, log the incident, and send an alarm to IDS MC.

The IDSM is a switching module designed for the Catalyst 6000 family of switches. When the Cisco Intrusion Detection System detects unauthorized network activity, the IDSM responds by generating an alarm that can be logged and displayed by IDS MC. The IDSM can terminate network connections when it is running sensor software version 3.0, and later, but not when it is running earlier versions.

Network sensing using either the sensor or the IDSM requires configuring a number of sensor (or IDSM) settings and signature settings. After configuring, tuning is required to achieve optimal performance, particularly to minimize false positives and false negatives.

Note Tuning sensor configurations should not be confused with tuning parameters for individual signatures.

Task List for Configuring Sensors and Signature Settings

Some settings can be configured only at the sensor level or only at the group level. For example, signatures can be configured only at the sensor level. As another example, identifying additional ports used by specific signatures can be done only at the group level. For step-by-step procedures on performing a specific task, refer to the corresponding section.

You initiate all these tasks in the Configuration > Settings TOC, which is shown in Figure 5-1 as it first appears when you select **Configuration > Settings**. Most of these tasks require you to use the Object Selector. The Object Selector handle appears to the left in Figure 5-1.

Figure 5-1 The Settings TOC

Tip The Configuration > Settings TOC and the Configuration > History page are the only places where the Object Selector is used in IDS MC.

Identifying Additional Ports Used by Specific Signatures Applied to a Sensor

When using IDSM devices supported by IDS MC, you can specify additional ports that should be considered by 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. These port settings also enable you to identify any custom TCP-based services, running across your internal networks, that you want the sensor to study for specialized attacks that target these network services.

Port mapping applies only to 3.x IDS modules, 4.x sensor appliances, and IDS MC groups. It does not apply to 3.x sensor appliances.

To identify additional or remapped ports for more extensive evaluation by specific signatures, follow these steps:

Step 1 Select **Configuration > Settings**.

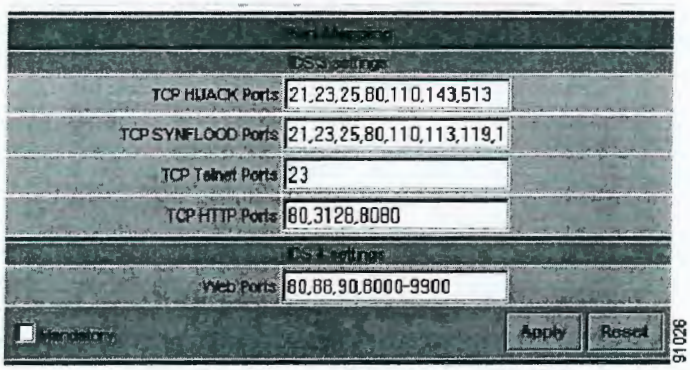
Step 2 Click the **Object Selector** handle.

Step 3 In the Object Selector, select the device or group for which you want to identify additional or remapped ports.

The Object Selector closes.

Step 4 In the TOC, select **Port Mapping**.

The Port Mapping page appears.



Step 5 To specify additional ports that should be considered by the signature that studies for hijacked ports on a TCP-based service, enter each port number in the TCP HIJACK Ports field, separating entries with a comma.

Step 6 To specify additional ports that should be considered by the signature that studies for TCP-based flood attacks, enter each port number in the TCP SYNFLOOD Ports field, separating entries with a comma.

Step 7 To specify additional ports that should be considered by the attack signature that studies for Telnet-based attacks, enter each port number in the TCP TELNET Ports field, separating entries with a comma.

Step 8 To specify additional ports that should be considered by the attack signature that studies for HTTP-based attacks, enter each port number in the TCP HTTP Ports field, separating entries with a comma.

Step 9 To accept your changes and close the Port Mapping page, click **Apply**.

Identifying Internal Networks

For each sensor or group of sensors that you manage with IDS MC, you can identify internal networks. These are networks that you consider trusted. Internal networks are handled differently from external networks for the purposes of reports and alarms.

To identify an internal network, follow these steps:

Step 1 Select **Configuration > Settings**.

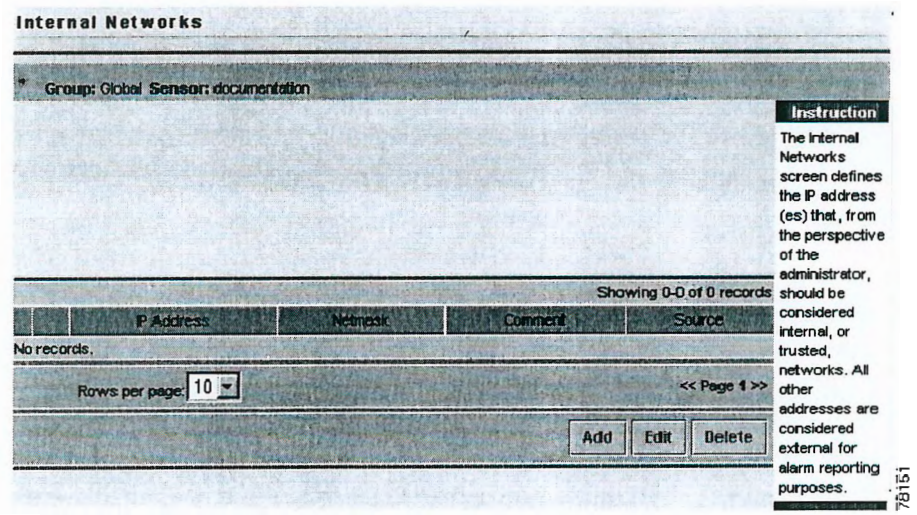
Step 2 In the TOC, click the **Object Selector** handle.

Step 3 In the Object Selector, select the sensor for which you want to identify an internal network.

The Object Selector closes.

Step 4 Select **Internal Networks**.

The Internal Networks page appears, and the Object bar displays the sensor you selected in the Object Selector.



Step 5 On the Internal Networks page, you can add an internal network. After you have added an internal network, you can edit its properties or delete it.

Configuring Link Status

For each sensor or group of sensors that you manage with IDS MC, you can configure the way that you want to see your link status reported by the Event Viewer in Security Monitor. Link status refers to the communication between a particular sensor or group of sensors and Security Monitor. You can specify how much time is to elapse before an interruption in your link is reported. You also can specify whether the interruption is to be regarded as an event of high, low, or medium severity.

You can perform this procedure for the sensor appliance but not for the IDSM.

To query for link status, follow these steps:

Step 1 Select **Configuration > Settings**.

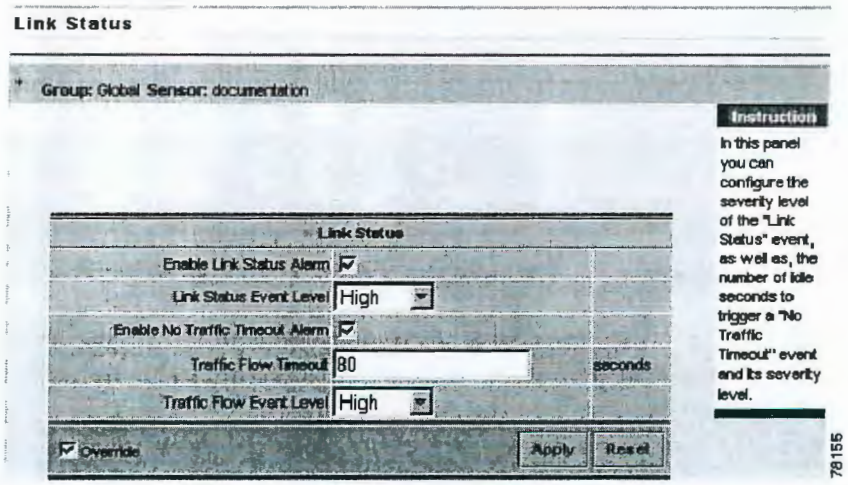
Step 2 In the TOC, click the **Object Selector** handle.

Step 3 In the Object Selector, select the sensor for which you want to configure the reporting of link status.

The Object Selector closes.

Step 4 Select **Link Status**.

The Link Status page appears, and the Object bar displays the sensor you selected in the Object Selector.



Step 5 On the Link Status page, you can specify global settings, or you can choose to override global settings.

Identifying Data Sources

A Cisco IOS router can publish syslog data to a sensor. You must specify the interface that the Cisco IOS router uses.

To identify the interface that a Cisco IOS router uses to publish syslog data to a sensor, follow these steps:

Step 1 Select **Configuration > Settings**.

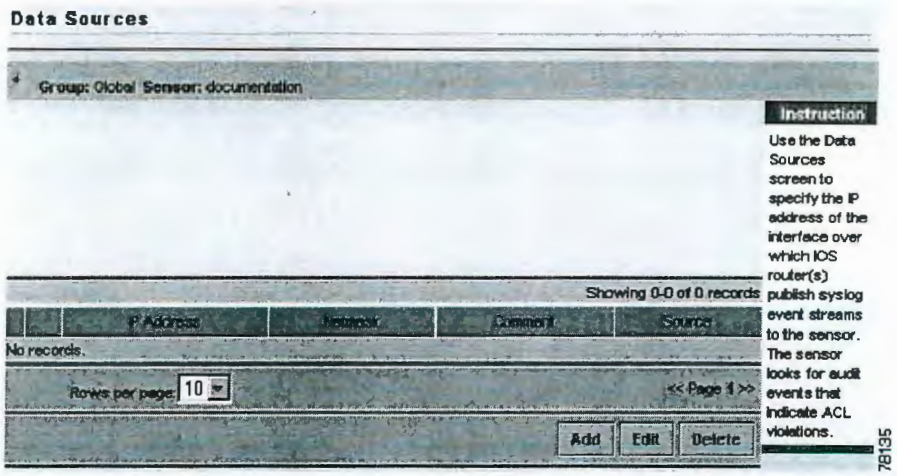
Step 2 In the TOC, click the **Object Selector** handle.

Step 3 In the Object Selector, select the sensor for which you want to specify a Cisco IOS router interface for the publication of syslog data.

The Object Selector closes.

Step 4 In the TOC, select **Data Sources**.

The Data Sources page appears, and the Object bar displays the sensor you selected in the Object Selector.



Step 5 On the Data Sources page, you can add an interface for syslog data publication by a Cisco IOS router. After you have added an interface, you can edit it or delete it.

Specifying Blocking Properties

You can configure a sensor to block an attack by generating ACL rules for publication to a Cisco IOS router. You can specify the blocking duration, the maximum number of ACL entries, whether to enable ACL logging, and whether to allow blocking devices to block the sensor's IP address.

You can remove blocking in the Event Viewer in Security Monitor.

To specify blocking properties, follow these steps:

Step 1 Select **Configuration > Settings**.

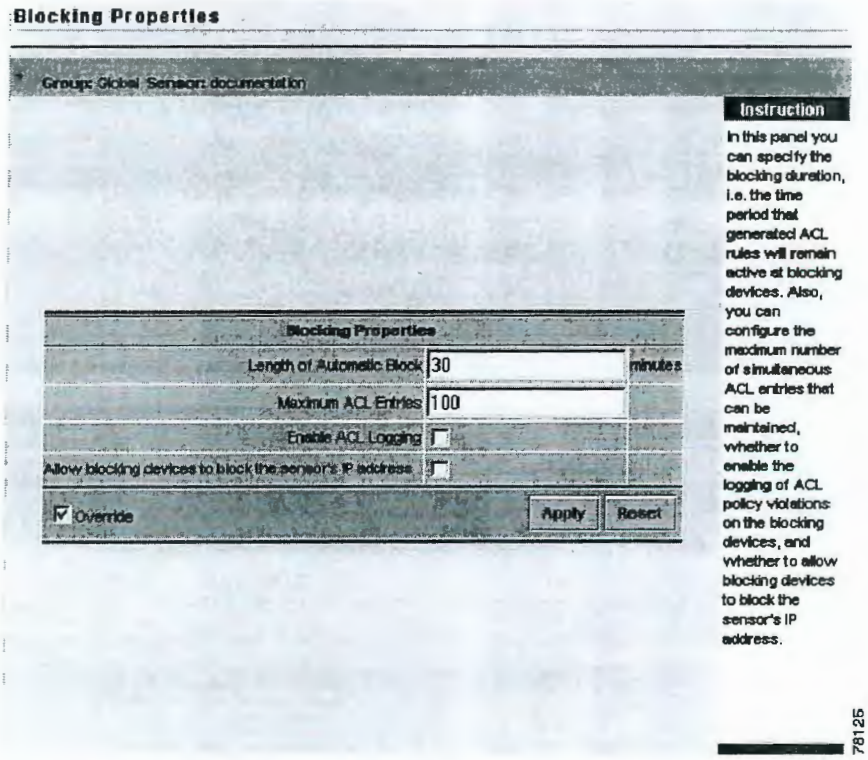
Step 2 In the TOC, click the **Object Selector** handle.

Step 3 In the Object Selector, select the sensor for which you want to specify blocking properties.

The Object Selector closes.

Step 4 In the TOC, select **Blocking Properties**.

The Blocking Properties page appears, and the Object bar displays the sensor you selected in the Object Selector.



Step 5 On the Blocking Properties page, you can specify global settings, or you can choose to override global settings.

Step 6 To remove blocking, use the Event Viewer in Security Monitor

Specifying Networks and Hosts that Should Never Be Blocked

You can configure a sensor to block an attack by generating ACL rules for publication to an Cisco IOS router. However, it is important to tune your sensor signatures to identify hosts and networks that should never be blocked. For example, you may have a trusted network device whose normal, expected behavior appears to be an attack. But such a device should never be blocked. Also, trusted, internal networks should never be blocked. Proper tuning reduces the number of false positives and helps ensure proper network operation.

To specify the networks or hosts that should never be blocked when an attack is detected, follow these steps:

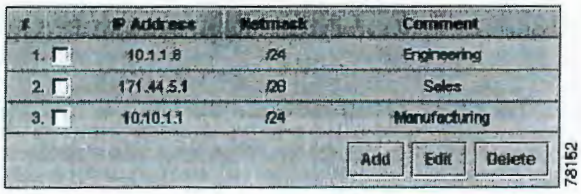
Step 1 Select **Configuration > Settings**.

Step 2 Click the **Object Selector** handle.

Step 3 In the Object Selector, select the sensor for which you want to identify hosts and networks that should be exempt from blocking.

Step 4 In the TOC, select **Blocking > Never Block Addresses**.

The IP Addresses page appears. This page shows the list of devices and networks that are capable of being blocked by configuring the sensor that you selected. On this page, you can add, edit, and delete hosts and networks.



Step 5 To add a host or network to the list of those that should never be blocked by the sensor that you selected, click **Add**.

The Enter Network page appears.

Enter the following information in the Enter Network page:

- IP address
- Network mask
- Comment

Step 6 To edit information associated with a host or network on the list of those that should never be blocked by the sensor that you selected, select the check box adjacent to the address of that host or network, and click **Edit**.

The Enter Network page appears.

Enter the following information on the Enter Network page:

- IP address
- Network mask
- Comment

Step 7 To delete a host or network from the list of those that should never be blocked by the sensor that you selected, select the check box corresponding to the address of that host or network, and click **Delete**.

The host or network that you selected is deleted.

Step 8 To add, edit, or delete additional hosts or networks, repeat Step 2 through Step 7.

Step 9 To continue configuring sensors, select **Configuration > Settings**.

Using Blocking Devices

You can configure a sensor to block an attack by generating ACL rules for publication to a Cisco IOS router. The Cisco IOS router in that situation is referred to as a *blocking device*. Before you can use a Cisco IOS router as a blocking device, you must identify it in IDS MC and specify its properties.

To identify a blocking device and specify its properties, follow these steps:

Step 1 Select **Configuration > Settings**.

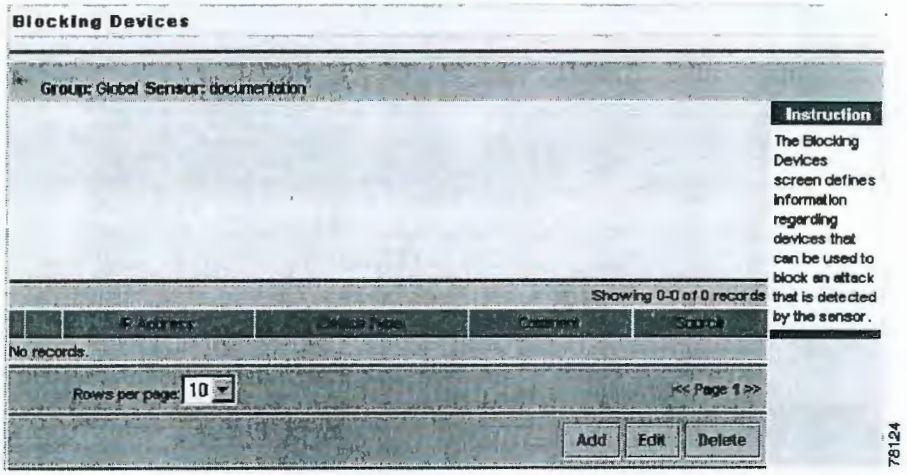
Step 2 In the TOC, click the **Object Selector** handle.

Step 3 In the Object Selector, select the sensor for which you want to specify a blocking device and its properties.

The Object Selector closes.

Step 4 In the TOC, select **Blocking Devices**.

The Blocking Devices page appears, and the Object bar displays the sensor you selected in the Object Selector.



Step 5 On the Blocking Devices page, you can add a Cisco IOS router to be used as a blocking device. After you have added a blocking device, you can edit it or delete it.

Specifying Master Blocking Sensors

A sensor can generate and apply ACL rules to block attacks that it detects. However, you may find that it is more effective in some configurations to have a proxy sensor generate and apply rules for attacks detected by another sensor on your network. These proxy sensors are referred to as *master blocking sensors*.

To specify master blocking sensors that should be used to block attacks detected by the selected sensor, follow these steps:

Step 1 Select **Configuration > Settings**.

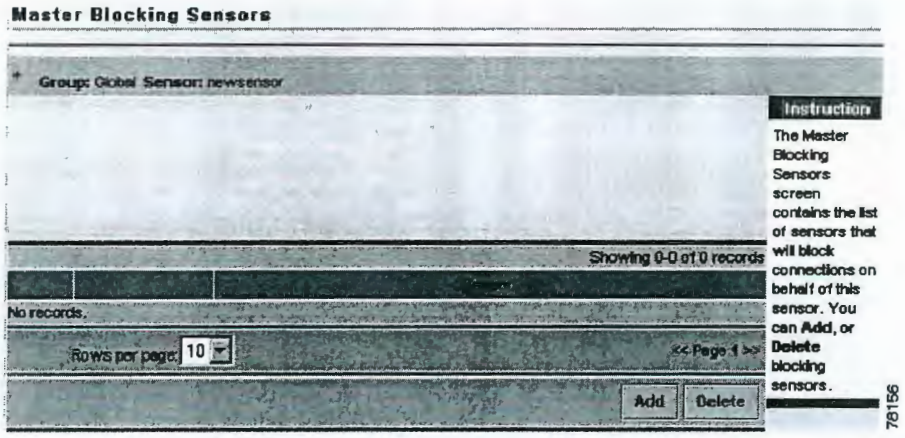
Step 2 In the TOC, click the **Object Selector** handle.

Step 3 In the Object Selector, select the sensor for which you want to specify a master blocking sensor.

The Object Selector closes.

Step 4 In the TOC, select **Master Blocking Sensors**.

The Master Blocking Sensors page appears, and the Object bar displays the sensor you selected in the Object Selector.



Step 5 To identify a master blocking sensor, click **Add**.

The sensor that you identify acts as a master blocking sensor.

Configuring Event Logging

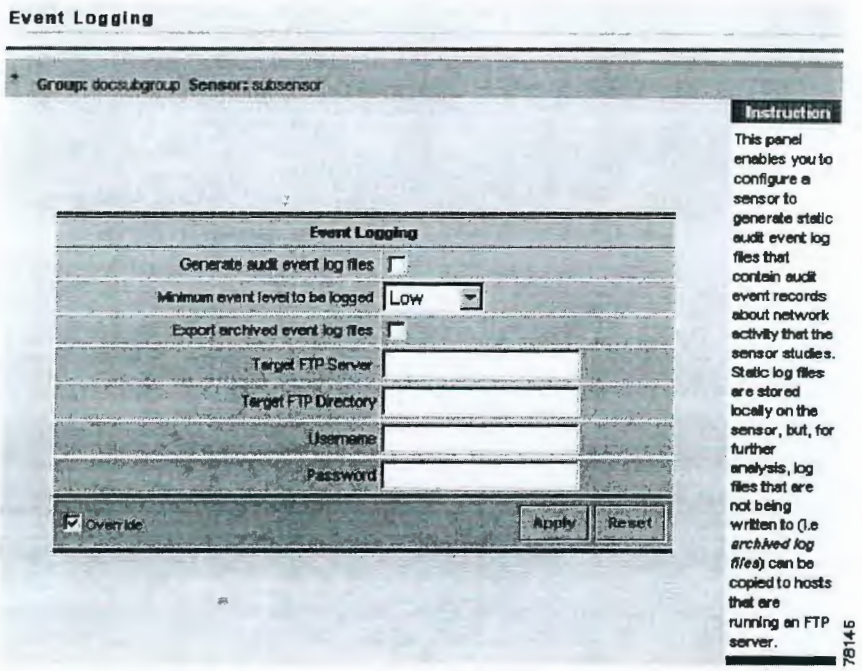
A sensor can generate audit event log files based on network data streams, or syslog data streams, or both, that the sensor is configured to study. The resulting log files are stored locally on the sensor.

To generate audit event log files, follow these steps:

Step 1 Select **Configuration > Settings**.

Step 2 In the TOC, select **Logging > Event Logging**.

The Event Logging page appears.



Step 3 On the Event Logging page, you can specify global settings, or you can choose to override global settings, by selecting the Override check box.

Step 4 To enable the generation of audit event log files, select the **Generate audit event log files** check box.

Step 5 Use the Minimum event level to be logged list box to set the minimum event level that you want to be logged.

Step 6 To specify an FTP server to which you want the sensor to publish a copy of the audit event log files that it archives (stops writing to after a new log file is created), select the **Copy archived event log files** check box.

Step 7 To specify the target FTP server, enter that server's IP address or DNS name in the Target FTP server field and press **Tab**.

Step 8 To specify the desired directory path on the target FTP server, enter that path in the Target FTP directory box and press **Tab**.

Step 9 To specify the user account that the sensor should use to log into the target FTP server, enter that user account in the Username field and press **Tab**.

Step 10 To specify the password that corresponds to the user account specified in the Username box, enter that password in the Password field.

The username/password pair is used to authenticate the sensor to the FTP server.

Configuring Automatic IP Logging

You can configure a sensor to generate an IP session log when the sensor detects an attack. If you want the sensor to take this action, you must specify it when you configure individual signatures. You must specify how long, in minutes, IP logging is to be done when a sensor detects an attack.

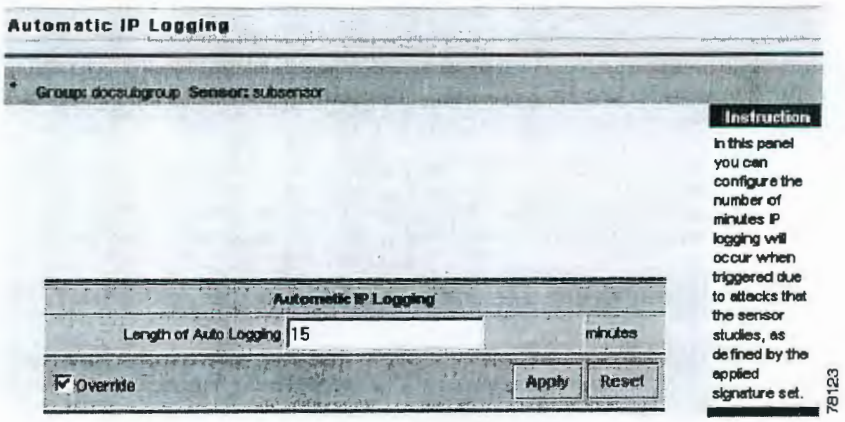
This procedure can be performed for the sensor appliance but not for the IDSM.

To specify the length of IP logging, follow these steps:

Step 1 Select **Configuration > Settings**.

Step 2 In the TOC, select **Logging > Automatic IP Logging**.

The Automatic IP Logging page appears.



Step 3 On the Automatic IP Logging page, you can specify global settings, or you can choose to override global settings, by using the Override check box.

Step 4 For a 3.x sensor, to specify the number of minutes that you want IP logging to be done, enter that value in the Length of Auto Logging box. Integer values from 1 through 60 are valid.

Step 5 For a 4.x sensor, you can specify additional logging parameters.

Step 6 To save your changes, click **Apply**.

Step 7 To discard your changes, click **Reset**.

Configuring IP Logging

You can configure a sensor to generate log files for specific IP addresses.

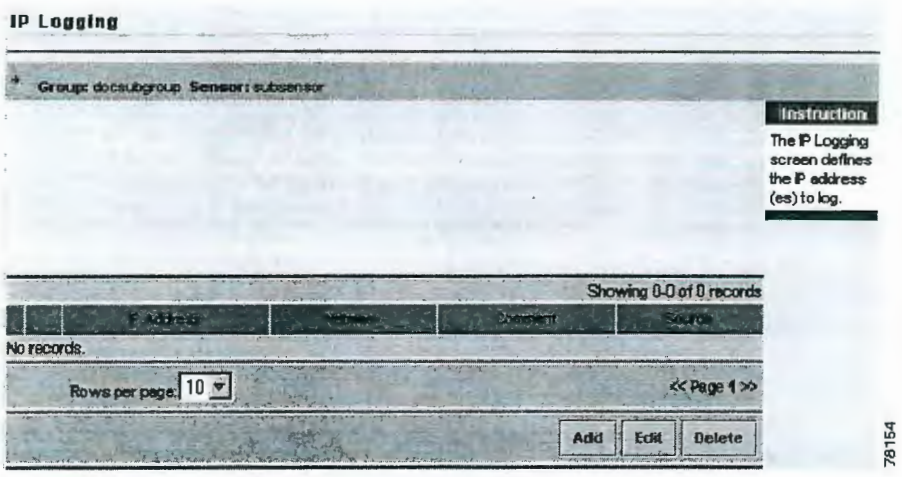
This procedure can be performed for the sensor appliance but not for the IDSM.

To generate log files for specific IP addresses, follow these steps:

Step 1 Select **Configuration > Settings**.

Step 2 In the TOC, select **Logging > IP Logging**.

The IP Logging page appears.



Step 3 On the IP Logging page, you can add an IP address for which you want to generate log files. After you have added an IP address, you can edit it or delete it.

Specifying Postoffice Settings

A sensor can monitor the services that are running on it. The sensor can generate audit events, as warnings, when a service goes down or cannot be restarted. This monitoring function, called Watchdog, helps you track the state and desired operation of your sensors. Watchdog is a feature of the postoffice service.

Watchdog checks the availability of services that are supposed to be running on the sensor and verifies that desired sensor-to-other network object communications (based on postoffice) are available. The Watchdog queries the services to see if they are operational, and if they are not, it issues warnings to the user and attempts to restart the services. You can specify the alarm levels of these warnings.

Additional postoffice settings that you can specify are the postoffice port and the heartbeat interval.

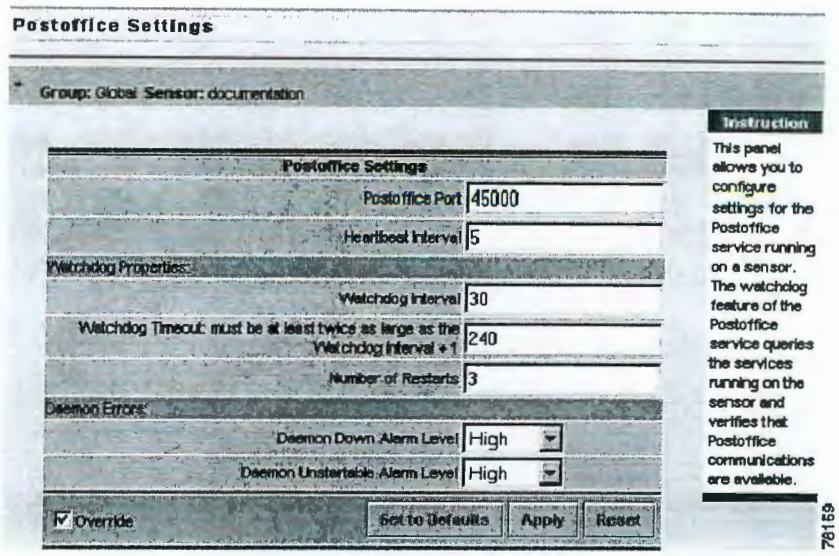
Note You will rarely need to modify the postoffice settings, and you should attempt to do so only if you are an expert user. Most users should not modify the default values.

To specify postoffice settings, follow these steps:

Step 1 Select **Configuration > Settings**.

Step 2 In the TOC, select **Communications > Postoffice Settings**.

The Postoffice Settings page appears.



Step 3 On the Postoffice Settings page, you can specify default settings, or you can choose to override default settings by using the Override check box.

Step 4 To specify a postoffice port other than the default value, enter the new value in the Postoffice Port field.

Step 5 To modify the interval that IDS MC uses to verify that all other postoffice clients with which it communicates are still accessible and available over the network, enter that value in the Heartbeat field.

To check client availability, IDS MC sends a postoffice packet to each known client and waits for a response packet. If the IDS MC postoffice does not receive a response, it assumes that the route to that client is no longer available, and postoffice issues a *route down* audit event. The heartbeat value is a whole number that represents how many seconds the postoffice running on IDS MC waits between each check for client availability.

Step 6 To specify how often (in seconds) the Watchdog feature should query the services that are supposed to be running on the sensor, enter that value in the Watchdog Interval field under Watchdog Properties.

Step 7 To specify how long the Watchdog feature should wait for a query response from the services that are supposed to be running on the sensor, enter that value in the Watchdog Timeout field.

Step 8 To specify how many times the Watchdog feature can attempt to restart a service that is determined to be inoperational, enter that value in the Number of Restarts field.

Step 9 To specify the level of the warning that should be issued when a service does not respond to the Watchdog query, select that value in the Daemon Down Alarm Level list box under Daemon Errors.

Step 10 To specify the level of the warning that should be issued when Watchdog cannot restart a service that is down, select that value in the Daemon Unstartable Alarm Level box.

Step 11 To discard your changes and restore the previous settings, click **Reset**.

Step 12 To save your changes, click **Apply**.

Specifying RDEP Properties

Version 4.x of IDS sensor software uses Remote Data Exchange Protocol (RDEP) instead of postoffice, which is used by earlier versions. RDEP, a subset of the HTTP/1.1 protocol, uses a client request/server response model. IDS MC does not use RDEP itself to communicate with the sensor. But it does allow the user to configure the RDEP properties on the sensor.

To specify RDEP properties, follow these steps:

Step 1 Select **Configuration > Settings**.

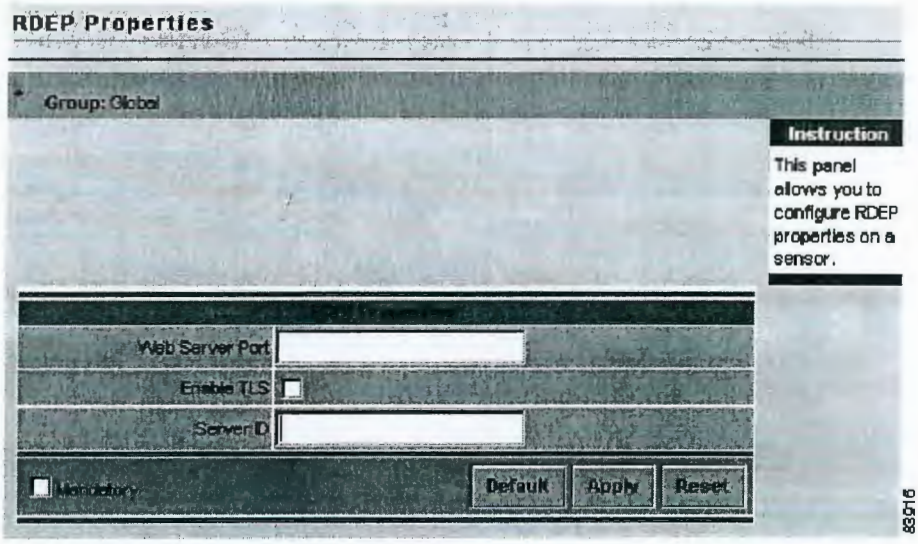
Step 2 In the TOC, click the **Object Selector** handle.

Step 3 In the Object Selector, select the sensor or group for which you want to specify RDEP properties. RDEP is available only with sensors and groups using Version 4.x of IDS sensor software.

The Object Selector closes.

Step 4 In the TOC, select **Communications > RDEP Properties**.

The RDEP Properties page appears, and the Object bar displays the sensor or group that you selected in the Object Selector.



Step 5 To use the properties of the parent group, deselect the **Override** check box. To enter properties that are different from those of the parent group, leave the **Override** check box selected.

Step 6 In the Web Server Port field, enter the port that the sensor uses for RDEP. (The sensor is the RDEP server, and the IDS MC server is the RDEP client.) The default value is 443 and normally does not need to be changed.

Step 7 Enter the Server ID to identify the web server on the sensor. The default value is HTTP/1.1 and normally should not be changed.

Step 8 Select **Enable TLS** to enable secure exchange between the RDEP server and the RDEP client. TLS (Transaction Layer Security) provides cipher and secret key negotiation, session privacy and integrity, and server authentication. This check box is selected by default.

Step 9 To discard your changes and restore the default values, click **Default**.

Step 10 To save your changes, click **Apply**.

Step 11 To discard your changes and restore the previous settings, click **Reset**.

Step 12 When specifying RDEP properties for a group instead of a sensor, you also have the option of making your settings mandatory. To make your settings mandatory, select the **Mandatory** check box.

Note By selecting the Mandatory check box, you ensure that your settings cannot be overridden by groups that are lower in the hierarchy of the Object Selector.

Adding Remote Hosts

This procedure applies to 3.x sensors. Unless you specify otherwise, the sensor will publish its audit event stream to the host on which you have installed IDS MC. You can identify additional network objects to which the sensor can publish its audit event stream. These additional network objects are referred to as *remote hosts* in IDS MC. A remote host can be any management client that is capable of processing the sensor's audit event stream, which uses postoffice-based network sessions.

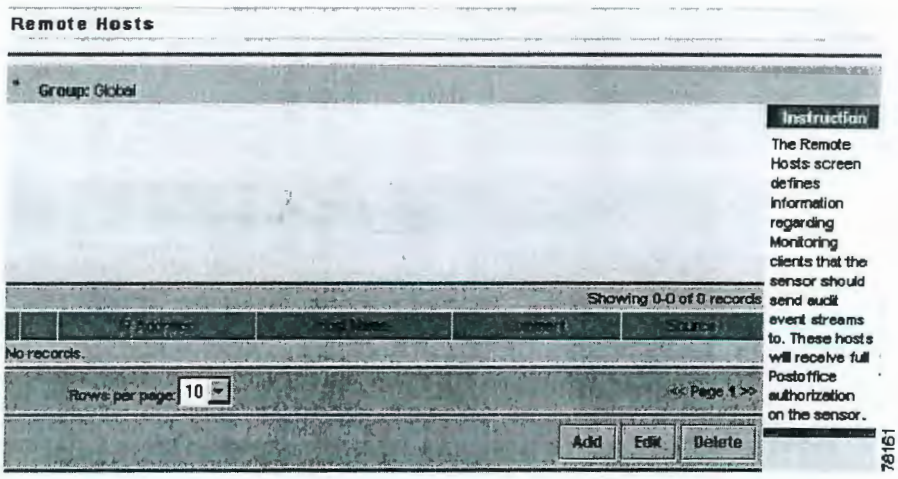
A sensor normally generates a notification and audit event record when it detects an attack. Using this procedure, you can set the minimum level of events to be reported to you. Setting the minimum level of events to be reported to you is one way that you can tune your signatures. Tuning your signatures reduces the number of false positives.

To specify remote hosts for a 3.x sensor, follow these steps:

Step 1 Select **Configuration > Settings**.

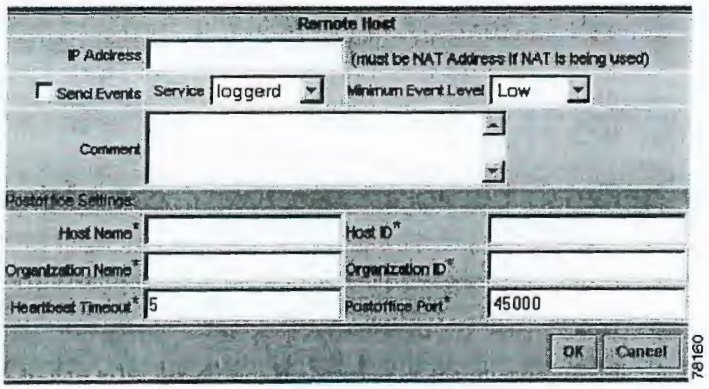
Step 2 In the TOC, select **Communications > Remote Hosts**.

The Remote Hosts page appears.



Step 3 To add a remote host, click **Add**.

The Remote Host page appears.



Step 4 Enter the IP address of the remote host in the IP Address field.

Step 5 To enable the sensor to send its audit event stream to the remote host whose IP address you just entered, select the **Send Events** check box.

Step 6 Specify the service in the Service list box. Four services, also called *daemons*, are available:

- loggerd
- eventd
- smid
- managed

Note More information on loggerd, eventd, smid, and managed is published in *Cisco Secure Intrusion Detection System Internal Architecture*, available at http://www.cisco.com/univercd/cc/td/doc/product/iaabu/csids/index.htm

Step 7 Set the minimum event level to be sent to the remote host in the Minimum Event Level list box.

You can select one of the following values:

- **Info**—Categorizes an event that is the result of standard activity on your network.
- **Low**—Categorizes the attack as mildly severe. These attacks are shown with a green icon in the Event Viewer in Security Monitor.
- **Medium**—Categorizes the attack as moderately severe. These attacks are shown with a yellow icon in the Event Viewer in Security Monitor.
- **High**—Categorizes the attack as highly severe. These attacks are shown with a red icon in the Event Viewer in Security Monitor.

Step 8 Enter a comment (optional).

Step 9 Enter the host name.

Step 10 Enter the host ID, which typically is the last octet of the IP address of the remote host.

Step 11 Enter the organization name and organization ID.

Note Use only lowercase letters to define organization names. Do not include spaces within the organization name. The host name and organization name are case-sensitive with respect to how postoffice processes audit events on the local host. Host names and organization names are not passed between different postoffice clients; only the Host ID and Org ID values are passed between different postoffice clients.

Note Within a postoffice domain, each organization ID/host ID pair must be unique. That is, no sensor, sensor group, or remote host can have the same organization ID/host ID pair as another sensor, sensor group, or remote host.

Step 12 To modify the interval that IDS MC uses to verify that all other postoffice clients with which it communicates are still accessible and available over the network, enter that value in the Heartbeat Timeout field.

To check client availability, IDS MC sends a postoffice packet to each known client and waits for a response packet. If the IDS MC postoffice does not receive a response, it assumes that the route to that client is no longer available, and postoffice issues a *route down* audit event. The heartbeat value is a whole number that represents how many seconds the postoffice running on IDS MC waits between each check for client availability.

Step 13 To specify a postoffice port other than the default value, enter the new value in the Postoffice Port field.

Step 14 To discard your changes and close the Remote Host page, click **Cancel**.

Step 15 To save your changes and close the Remote Host page, click **OK**.

The Remote Host page appears, showing the remote host that you just added.

Step 16 After you have added a remote host, you can edit its properties or delete it.

Identifying Allowed Hosts

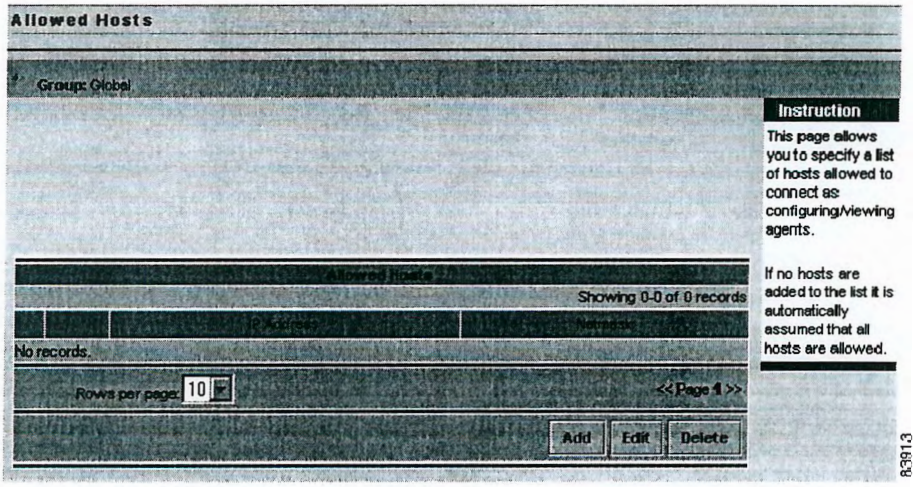
This procedure applies to 4.x sensors. Unless you specify otherwise, all hosts on your network are allowed to connect to a sensor to configure it and receive alarm data from it. However, you can identify allowed hosts; if you do, no other hosts will be allowed to connect to a sensor.

To identify allowed hosts for a 4.x sensor, follow these steps:

Step 1 Select **Configuration > Settings**.

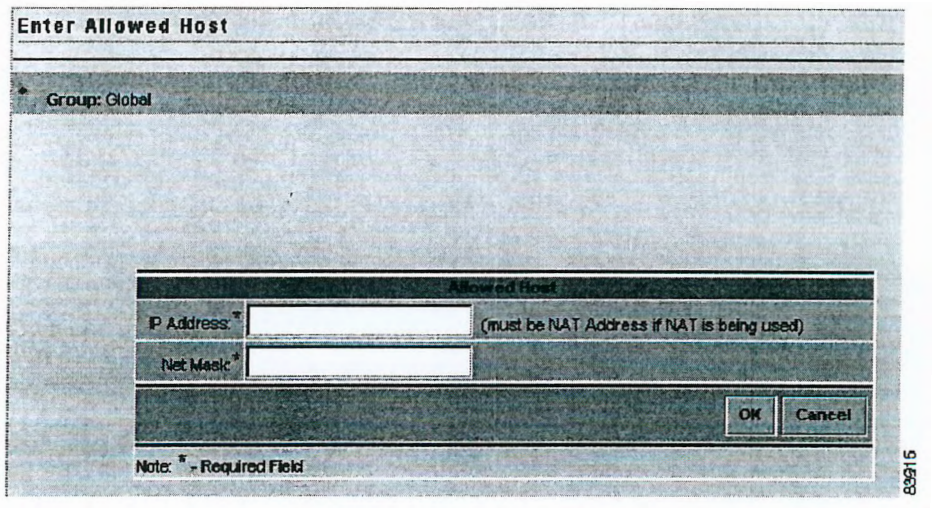
Step 2 In the TOC, select **Communications > Allowed Hosts**.

The Allowed Hosts page appears.



Step 3 To add a remote host, click **Add**.

The Enter Allowed Host page appears.



Step 4 Enter the IP address of the allowed host in the IP Address field.

Step 5 Enter the net mask of the allowed host in the Net Mask field.

Step 6 To discard your changes and close the Enter Allowed Host page, click **Cancel**.

Step 7 To save your changes and close the Enter Allowed Host page, click **OK**.

Using Additional Settings

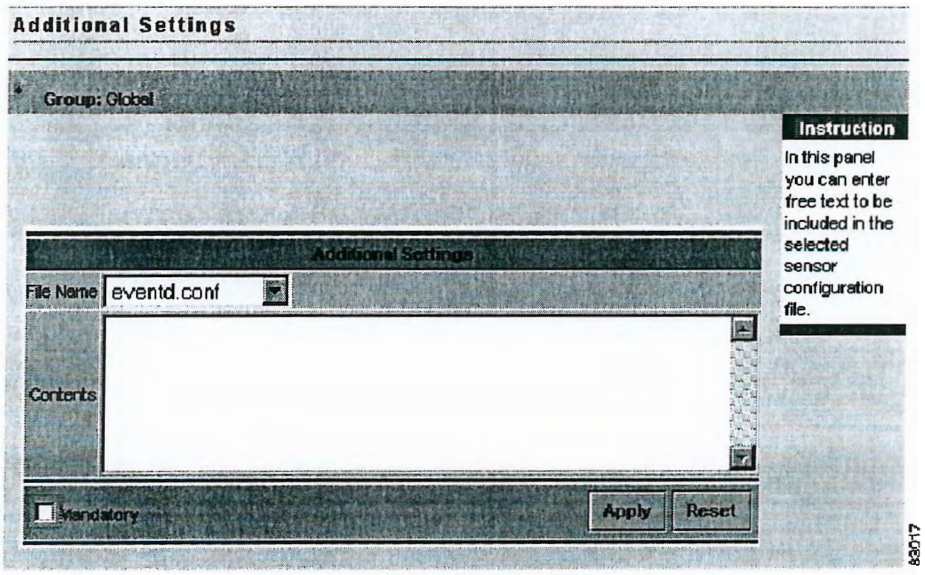
This procedure applies to 3.x sensors. Configuration file settings that are not supported by IDS MC can be entered manually, as text input.

To enter additional settings for a 3.x sensor, follow these steps:

Step 1 Select **Configuration > Settings**.

Step 2 In the TOC, select **Advanced > Additional Settings**.

The Additional Settings page appears.



Step 3 Select the sensor configuration file to which you want to add additional text in the File Name list box.

Step 4 In the Contents field, enter the text you want to add to the sensor configuration file that you selected.

Step 5 To discard your changes and restore the previous settings, click **Reset**.

Step 6 To save your changes, click **Apply**.

Step 7 To make your settings mandatory, select the **Mandatory** check box.

Note By selecting the Mandatory check box, you ensure that your settings cannot be overridden by devices that are lower in the hierarchy of the Object Selector.

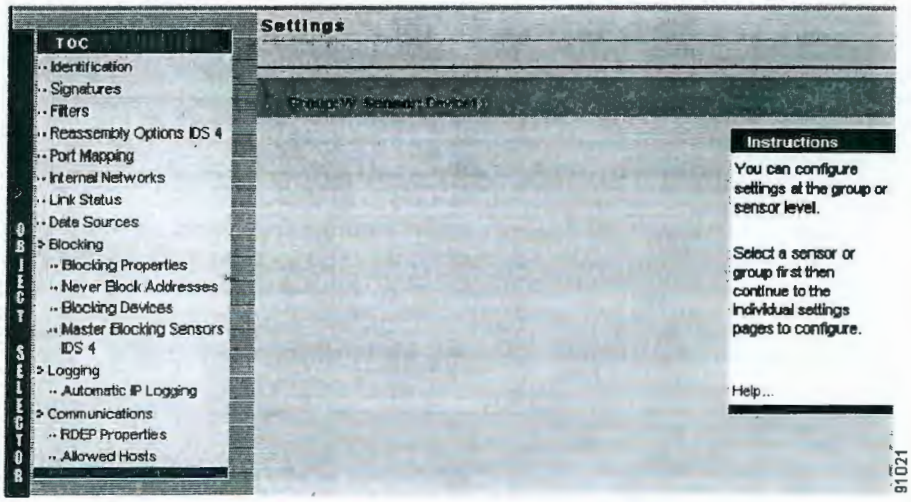
Defining Identification Properties for a Sensor

You can change the properties of a sensor that you have already added to your network. However, some properties cannot be changed.

To define identification properties for a sensor, follow these steps:

Step 1 Select **Configuration > Settings.**

The Settings page and TOC appear; 4.x sensors appear as shown here.



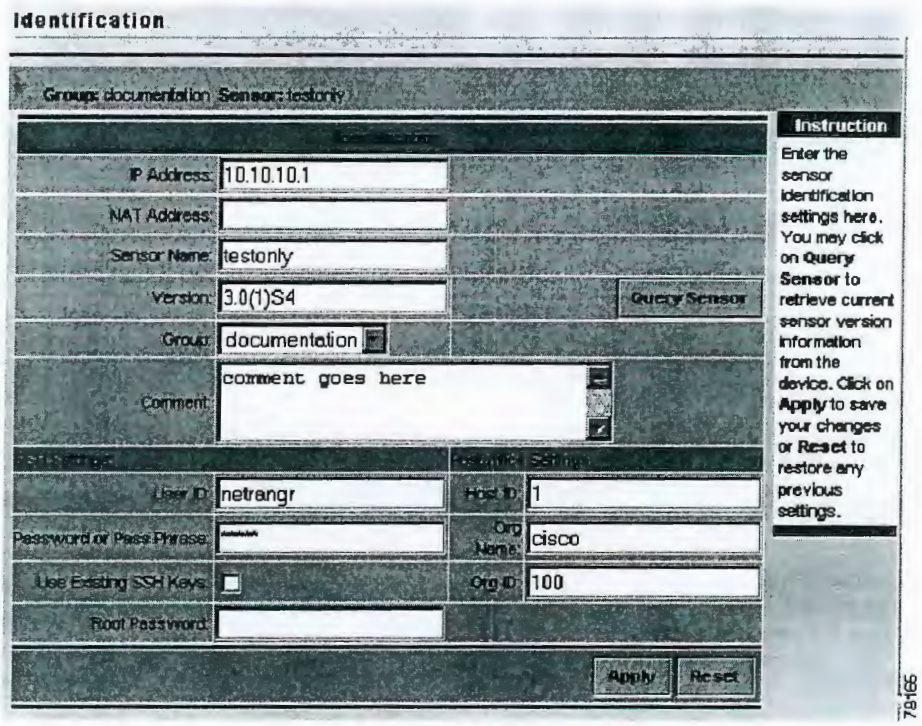
Step 2 In the TOC, click the **Object Selector** handle.

Step 3 In the Object Selector, select the sensor for which you want to define identification properties.

The Object Selector closes.

Step 4 In the TOC, select **Identification**.

The Identification page appears, and the Object bar displays the sensor you selected in the Object Selector. The properties of the sensor also appear. The Identification page appears as shown here for 3.x sensors; 4.x versions do not have fields for Root Password or Postoffice Settings.



Step 5 To determine which version of sensor software is installed on the sensor, click **Query Sensor**; this action will update the information displayed by the Identification page if necessary. If you then click **Apply**, and the queried version is different from the current version, the configuration will be upgraded to the new version. If you click **Cancel**, no changes will be applied.

Step 6 On the Identification page, make any desired changes to the values in the IP Address, NAT Address, Sensor Name, and Comment fields. You can change the group that the sensor belongs to by using the Group list box. You cannot change the value in the Version field on this page.

Step 7 On the SSH Settings page, you can choose to use a password or to use existing SSH keys for Secure Shell (SSH) communications between your host and the sensor.

- **Password**—To use this option, enter your user ID and password.
- **Existing SSH Keys**—To use this option, enter your user ID and select the **Use Existing SSH Keys** check box.

Step 8 In the Postoffice Settings content area, enter the postoffice settings of the sensor: Host ID (typically the last octet of the IP address of the sensor), Org Name (all lowercase letters and no spaces), and Org ID (default value 100).

Within a postoffice domain, each Org ID/Host ID pair must be unique. That is, no sensor or sensor group can have the same Org ID/Host ID pair as another sensor or sensor group.

Note You should use only lowercase letters to define organization names. Additionally, do not include spaces within the organization name. The host name and organization name are case sensitive with respect to how postoffice processes audit events on the local host. Host names and organization names are not passed between different postoffice clients, only the Host ID and Org ID values.

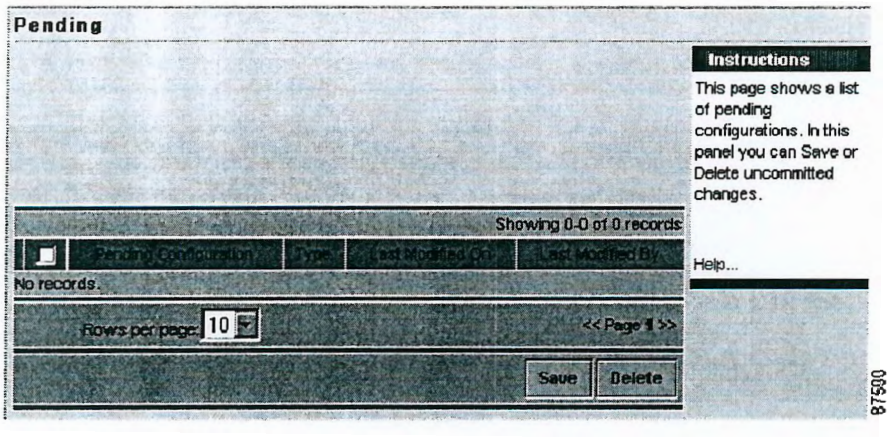
Step 9 To discard your changes and restore the previous settings, click **Reset** and skip the rest of this procedure.

Step 10 To save your changes, click **Apply**.

Caution Your changes will have no effect on your sensor configuration until you commit them to the database.

Step 11 To see the identification properties you just changed, select **Configuration > Pending**.

The Pending page appears, showing the device whose identification properties you just changed:



Step 12 To delete a pending configuration without committing it to the database, select the check box for the configuration that you want to delete and click **Delete**.

Step 13 To commit a pending configuration to the database, select the check box for the configuration that you want to commit to the database and click **Save**.

Learn More About Signatures

Network intrusions can be defined as attacks or other misuses of network resources. Cisco IDS sensors use a *signature-based* technology to detect network intrusions. A *signature* specifies the types of network intrusions that you want the sensor to detect and report. A signature can be thought of as 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.

On a basic level, *signature-based* intrusion detection technology can be compared to virus-checking programs. Cisco Systems produces a list of signatures that the sensor compares with network activity. When a match is found, the sensor takes some action, such as logging the event or sending an alarm to the Event Viewer provided with Monitoring Center for Security (Security Monitor). Sensors allow

users to modify existing signatures and define new ones. However, most customers depend on Cisco Systems to provide the latest signatures to keep the sensor up to date and thus able to detect the latest attacks.

Tip To be informed about the latest signatures by e-mail, you can subscribe to the Cisco IDS Active Update Notification. The subscription form is available at http://www.cisco.com/warp/public/779/largeent/it/ids_news/subscribe.html.

Signature-based intrusion detection can produce false positives, because certain normal network activity can be construed as malicious. 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.

Sensors can be configured to take one or more of three actions in addition to generating alarms:

- **IP Log**—This action writes the IP session data to a file. By default, this action is not taken. The IP log action is not available when using the IDSM. It is available only when using the sensor appliance.
- **Reset**—This action sends a TCP reset command to the session in which the attack signature was detected. By default, this action is not taken. The reset action is available only for TCP-based attack signatures. The reset action is not available when using the IDSM. It is available only when using the sensor appliance.
- **Block**—This action causes the sensor to issue commands to a router to block any source addresses from sending traffic that matches an attack signature. These commands are issued as temporary ACL statement changes to the router configuration. After a specified period of time, the sensor removes those statements, restoring the router to its pre-attack configuration.

Signatures can be categorized and grouped in several different ways, some of which are the following:

- *Embedded* signatures are included in the sensor software. You cannot add to or delete from the list of embedded attack signatures. You also cannot rename them. The list of embedded signatures available to a sensor depends upon the version of software the sensor is running. You can find more information about embedded signatures in the Cisco Network Security Database. To view the Network Security Database, open your web browser to https://*host name*/vms/nsdb/html/all_sigs_index.html, where *host name* is the name of the computer where IDS MC is installed.
- *TCP Connection* signatures are user-configurable signatures based on the transport-layer protocol (TCP) and port number of the traffic being monitored. *UDP Connection* signatures are user-configurable signatures based on the transport-layer protocol (UDP) and port number of the traffic being monitored.
- *String-matching* signatures are user-configurable signatures based on data carried by the packets, that is, the content of a particular session. String-matching signatures use regular expressions to perform string matching on the packet data payload. Furthermore, string-matching signatures can be configured to examine only incoming, outgoing, or bidirectional network traffic for the string.
- *ACL violation* signatures are user-configurable signatures based on access control violations recorded by network devices in the syslog stream. To configure the sensor to detect ACL signatures, you must first configure one or more routers to log ACL violations. Then, you must configure the router to communicate with the sensor, and configure the sensor to accept syslog traffic from the router.
- *Custom* signatures are user-defined signatures that allow a maximum degree of tuning through signature engine parameters. Custom signatures on the sensor appliance, but not on the IDS module, can be tuned. More information on signature engine parameters is available in *Cisco Intrusion Detection System Signature Engines Version 3.0* at http://www.cisco.com/univercd/cc/td/doc/product/iaabu/csids/csids6/index.htm

Configuring and Tuning Signatures

You can configure the following properties of signatures:

- **Severity**—Categorizes the attack. The severity setting is used in Event Viewer in Security Monitor to distinguish among the types of attacks being logged.
- **Enabled**—Configures the sensor to scan network traffic for that particular signature and to generate an alarm when an attack is detected. Disabling a signature causes the sensor to disregard any network traffic that displays the signature.
- **Action**—Determines the action or actions the sensor will take, in addition to generating an alarm, when it detects an attack.
- **Signature Name**—Used when adding a new signature (not used for all categories and groupings of signatures).
- **Signature ID**—The ID of the signature, which is generated by IDS MC and is a value that you cannot change (used only for custom signatures).
- **Subsig ID**—Specifies the subsignature ID (not used for all signatures). For example, every string-matching signature has a subsignature ID, which is generated by IDS MC and is a value that you cannot change. Also, every ACL violation signature has a subsignature ID, which is generated by IDS MC and is a value that you cannot change; when you create a new ACL violation signature, the Subsig ID field will be populated with a value that is greater by 1 than the subsignature having the highest number in the list.
- **Port**—Used to set the port number (not used for all categories and groupings of signatures; used, for example, for TCP connection signatures, UDP connection signatures, and string-matching signatures).
- **ACL Name**—Specifies the name or number of the ACL to be monitored (used only for ACL violation signatures).
- **String**—Specifies the string to be matched. The string is in the form of a regular expression (used only in string-matching signatures).
- **Direction**—Specifies the direction of the traffic to be monitored (not used for all categories and groupings of signatures).
- **Occurrences**—Specifies the number of times a particular string is to be detected before the sensor generates an alarm (not used for all categories and groupings of signatures).

Some signatures can be tuned. Tuning signature parameters should not be confused with tuning sensor configurations.

Some signatures have special characteristics:

- Embedded signatures cannot be added, deleted, or renamed, because they are provided with the sensor software itself. Embedded signatures are found in the General grouping of the Signature ID category for both 3.x and 4.x sensors.

  The information for embedded signatures, such as their names and IDs, appears as it does in the Cisco Network Security Database (NSDB). To view the NSDB from the Signatures page, click a signature ID, such as 2000, in the ID column. The entries in the ID column are hyperlinks to the NSDB.

- When using a 3.x sensor, you can rename, modify, or delete any default TCP connection signature, and you can add TCP connection signatures as needed. However, you cannot create duplicate TCP connection signatures. A duplicate TCP connection signature has the same port number as another TCP connection signature.

- When using a 3.x sensor, you can rename, modify, or delete any default UDP connection signature, and you can add UDP connection signatures as needed. However, you cannot create duplicate UDP connection signatures. A duplicate UDP connection signature has the same type and port number as another UDP connection signature.

- When using a 3.x sensor, you can rename, modify, or delete any default string-matching signature, and you can add string-matching signatures as needed. However, you cannot create duplicate string-matching signatures. A duplicate string-matching signature has the same string, port, and direction as another string-matching signature.

- For 3.x sensors, there are no default ACL violation signatures provided when configuring a sensor for the first time. You must create ACL violation signatures, and you can modify them after you create them. However, you cannot create a duplicate ACL violation signature. A duplicate ACL signature is defined as an ACL signature with the same ACL name or subsignature ID as another ACL violation signature.

- No custom signatures are provided with a new 3.x sensor or a new 4.x sensor. You can create custom signatures and modify any existing custom signatures. However, you cannot create a duplicate custom signature. A duplicate custom signature is defined as a custom signature with the same ID as another custom signature.

Some signatures have special requirements. For example, to configure a sensor to detect ACL violation signatures, you must first configure one or more Cisco IOS routers to log ACL violations. Then, you must configure those routers to communicate with the sensor. Finally, you must configure the sensor to accept syslog traffic from those routers. You can configure the following properties for each ACL signature:

To configure a signature, follow these steps:

Step 1 Navigate to the Signatures page and select a particular signature to configure, if desired:

a. Select **Configuration > Settings**.

b. In the TOC, click the **Object Selector** handle.

c. In the Object Selector, select the sensor for which you want to configure a signature.

The Object Selector closes.

d. In the TOC, select **Signatures**.

The Signatures page appears, and the Object bar displays the sensor you selected in the Object Selector.

Notice that the Group Signatures list box displays the Signature ID category. You can also use the Group Signatures list box to display the L2/L3/L4 Protocol Signatures, Service Signatures, Attack Signatures, and OS Signatures categories. This is true for both 3.x sensors and 4.x sensors.

For 3.x sensors, the Signature ID category contains the groupings General, TCP Connection, UDP Connection, String Match, ACL Violation, and Custom. For 4.x sensors, the Signature ID category contains the groupings General and Custom.

For 3.x sensors, *General* means embedded; embedded signatures are part of the sensor software. For 4.x sensors, *General* means all signatures other than those that you create.

e. Continue using the categories and groupings to select a signature to configure.

Tip You can filter the display of the signature table. Using the Filter Source list, select any of the displayed columns as the filter source. Next, enter a value in the adjacent field and click **Filter**. For example, select **Severity** in the list box and enter the value **High** in the adjacent field. When you click **Filter**, the signature table displays all signatures that have a high severity. Clearing the search string or entering the wildcard character ("*") cancels filtering. Note that this filter is not the same as Filters in the Configuration > Settings TOC.

Step 2 Enable or disable all signatures in a particular grouping, if desired:

a. In the category you want, such as Signature ID for 3.x sensors, select a grouping, such as General.

b. To enable all the signatures in, for example, the General grouping, select the check box corresponding to general signatures and click **Enable**. By default, the most critical signatures are enabled when you install IDS MC.

Step 3 Configure one or more signatures in a particular grouping, if desired:

a. In the category you want, such as Signature ID for 3.x sensors, select a grouping, such as General.

The Signature(s) in Group page appears, and the Object bar displays the group name and sensor name. Notice that the Signature Group list displays General in this example.

b. Select the check box corresponding to the signature that you want to configure. *Configure* in this context means to enable or disable, set severity, and select an action.

Timesaver You can select more than one check box but you cannot configure as many properties if you do.

Tip You can select all signatures by selecting the check box in the heading of the signature table. Also, you can sort a column by clicking the title of the column.

c. Click **Edit**.

The Edit Signature(s) page appears, showing the name of the signature that you selected. Depending upon the category and grouping of signature that you are configuring, the Edit Signature(s) page will have different fields.

d. To edit a signature name (not possible for all categories and groupings of signatures), make changes in the Signature field.

e. To disable a signature that is enabled, deselect the **Enable** check box. To enable a signature that is disabled, select the **Enable** check box.

f. To change the severity of a signature, use the Severity list box. You can select one of the following values for each signature:

- **Info**—Categorizes an event that is the result of standard activity on your network.
- **Low**—Categorizes the attack as mildly severe. These attacks are shown with a green icon in the Event Viewer in Security Monitor.
- **Medium**—Categorizes the attack as moderately severe. These attacks are shown with a yellow icon in the Event Viewer in Security Monitor.
- **High**—Categorizes the attack as highly severe. These attacks are shown with a red icon in the Event Viewer in Security Monitor.

g. To specify the action (or actions) that you want the sensor to take upon detecting a particular attack, select one or more of the following check boxes.

Note Some actions are not available to certain versions of sensor software.

- **Block**—The sensor issues a command to a PIX Firewall, a Cisco router, a Catalyst 6000 switch, or another supported device. That device then denies the host or network from which the attack originated entry to the monitored network.
- **TCP Reset**—The sensor resets the TCP session in which the attack signature was detected. Reset is available only to TCP-based attack signatures. If not available, this action is dimmed.
- **IP Log**—The sensor generates an IP session log with information about the attack. This action is not available in all versions of sensor software. If not available, this action is dimmed.

h. To edit the string (only for string-matching signatures), make changes in the String field.

Caution The regular expression you enter here is not compiled by a regular expression compiler. Therefore, you must be careful to enter a valid regular expression; it is *not validated here.*

i. To edit the number of occurrences of the string that will cause the sensor to generate an alarm (only for string-matching signatures), make changes in the Occurrences field.

j. To edit the port number (not used for all signatures), make changes in the Port field.

k. To edit the ACL name or number (used only for ACL violation signatures), make changes in the ACL Name field.

l. To edit the direction of the traffic to be monitored (not used for all signatures), use the Direction list box. You can select one of the following values:

- **To**—Specifies that incoming packets should be searched for the defined string.
- **From**—Specifies that outgoing packets should be searched for the defined string.
- **Both**—Specifies that both incoming and outgoing packets should be searched for the defined string.

m. To accept your changes and close the Edit Signature(s) page, click **OK**.

The Signature(s) in Group page appears, showing the changes that you just made.

Step 4 Tune a particular signature, if desired:

Note Not all signatures can be tuned. If a particular signature does not have an entry in the Engines column, that signature cannot be tuned. Also, signatures that use the engine named `Other` cannot be tuned.

a. In the category you want, such as Signature ID for 4.x sensors, select a grouping, such as General.

b. Select the Engine Name corresponding to the signature that you want to tune.

The Tune Signature page appears, showing the name of the signature that you selected. On this page, for the engine that you selected, you can edit parameters or set them to their default values.

Clicking **Default** retrieves the built-in micro-engine parameter information for the signature that you are tuning. You can then adjust the default values if needed. Note that only deviations from the built-in micro-engine parameter information are saved by IDS MC, because only such deviations need to be saved.

More information on signature engine parameters is in *Cisco Intrusion Detection System Signature Engines Version 3.0*: http://www.cisco.com/univercd/cc/td/doc/product/iaabu/csids/csids6/index.htm.

c. To accept your changes and close the Tune Signature page, click **OK**.

The Signature(s) in Group page appears.

Step 5 Add a signature, if desired:

Note Not all categories and groupings of signatures can have signatures added to them. As examples, you can add custom signatures, string-matching signatures, UDP connection signatures, and TCP connection signatures.

a. In the category you want, such as Signature ID for 4.x sensors, select a grouping, such as Custom.

The Signature(s) in Group page appears, and the Object bar displays the group name and sensor name. Notice that the Signature Group list displays Custom in this example.

b. Click **Add**.

The Tune Signature page appears.

c. Enter the name of the signature that you want to add.

d. Select a signature engine in the Engine list box.

e. Tune the new signature as described in Step 4 of this procedure.

f. Configure the new signature as described in Step 3 of this procedure.

Defining Filters for a Sensor

Filters can be used to reduce the number of false positives reported by your sensors, so they are considered a method of tuning your sensors.

Filtering an alarm means that the sensor will analyze the data stream but will not generate an alarm. Filtering all alarms from a particular signature is not the same thing as disabling that signature, which results in no analysis of the data stream for that signature.

Note Filters for a sensor in IDS MC should not be confused with event filters that are part of an event rule in Security Monitor.

A filter is defined by specifying the signature, the source address, and the destination address and whether it is an inclusive or exclusive filter. You cannot define any particular part of the filter (such as the source address) as inclusive or exclusive; you have to define the entire filter as inclusive or exclusive. Also, if you define more than one filter, IDS MC will apply them in the order in which you defined them.

An example of how filters work can be helpful in seeing how to define them. In this example, you want to exclude all alarms that originate from Network 10.10.10.0/24 because that network is using some applications that generate large numbers of false positives. However, there are two signatures that are important to you, so you don't want them to be excluded: They are 994 (Traffic Flow Started) and 995 (Traffic Flow Stopped).

1. Begin by defining an exclusive filter. Specify the source address as 10.10.10.0, which is the network that is generating large numbers of false positives. Specify all signatures so that no alarms are sent to Security Monitor.
2. Next, define an inclusive filter. Specify the same source address, which is Network 10.10.10.0. But specify Signatures 994 and 995, which are the ones that you want to include because they are important to you.

By using these two filters, and in this order, you can filter out a large number of alarms that would be false positives. But you can selectively let some of them (Signatures 994 and 995) pass through. This is possible because you defined the exclusive filter first and the inclusive filter next. Note that if you had defined the inclusive filter first, then the exclusive filter would have filtered out all the alarms from Network 10.10.10.0. This is because filters are evaluated in order.

This procedure defines filters for a sensor as described in this example. The example assumes that you have added Device11 in GroupW to your network. Device11 is a 4.x appliance sensor in this example.

To define a filter for a sensor as described in the example, follow these steps:

Step 1 Select **Configuration > Settings**.

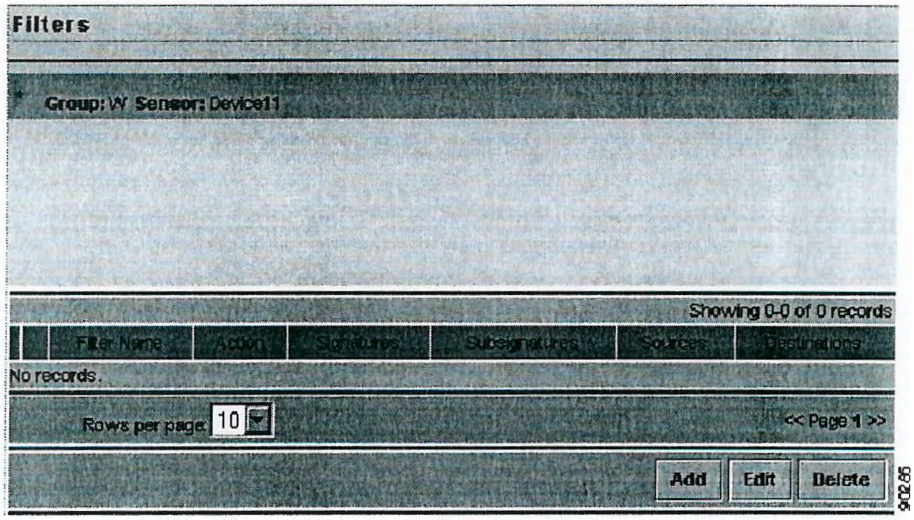
Step 2 In the TOC, click the **Object Selector** handle.

Step 3 In the Object Selector, select Device11, the sensor for which you want to define a filter in this example. Device11 is a 4.x sensor.

The Object Selector closes.

Step 4 In the TOC, select **Filters**.

The Filters page appears. This page shows that no filters have been defined for Device11, the sensor that you selected.



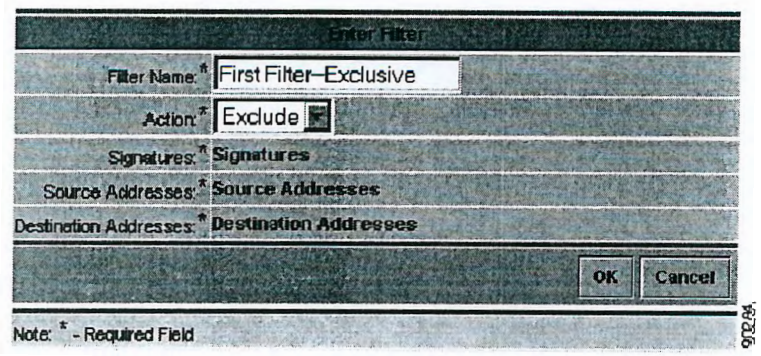
Step 5 To begin defining the exclusive filter in this example, click **Add**.

The Enter Filter page appears.

Step 6 Enter a name for the filter: Use "First Filter--Exclusive"

Step 7 Select the action of **Exclude**.

The Enter Filter page now appears as shown here.

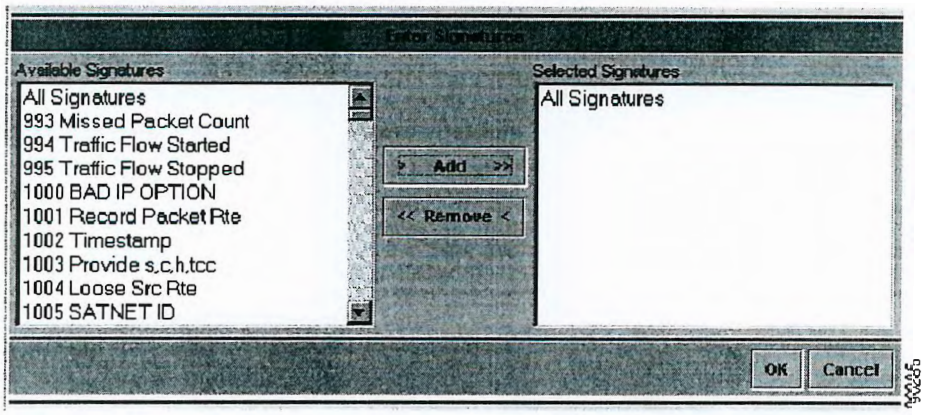


Step 8 Click the **Signatures** link.

The Enter Signatures page appears.

Step 9 On the Enter Signatures page, add **All Signatures** from the Available Signatures field to the Selected Signatures field.

The Enter Signatures page now appears as shown here.



Step 10 Click **OK**.

The Enter Filter page appears again.

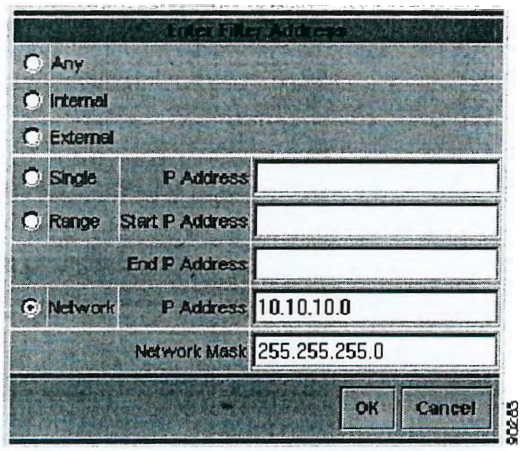
Step 11 Click the **Source Addresses** link.

The Filter Source Addresses page appears.

Step 12 Click **Add**.

The Enter Filter Address page appears.

Step 13 Select the radio button corresponding to Network and enter 10.10.10.0, the network address being used in this example, along with its network mask of 255.255.255.0. The **Enter Filter Address** page now appears as shown here.



Step 14 Click **OK**.

Step 15 The Filter Source Addresses page appears, showing the addition of Network 10.10.10.0 with a subnet mask of 255.25.255.0.

Step 16 Click **OK**.

The Enter Filter page appears again.

Step 17 Click the **Destination Addresses** link.

The Filter Destination Addresses page appears.

Step 18 Click **Add**.

The Enter Filter Address page appears.

Step 19 Select the radio button corresponding to an address of Any and click **OK**.

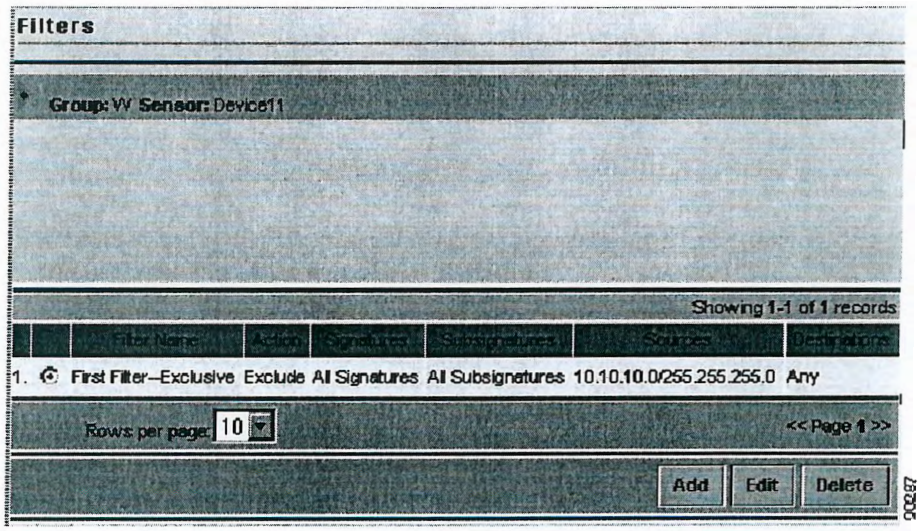
The Filter Destination Addresses page appears, showing the addition of Any.

Step 20 Click **OK**.

The Enter Filter page appears again.

Step 21 Click **OK**.

The Filters page now appears as shown here. You have just finished defining the first filter in this example.

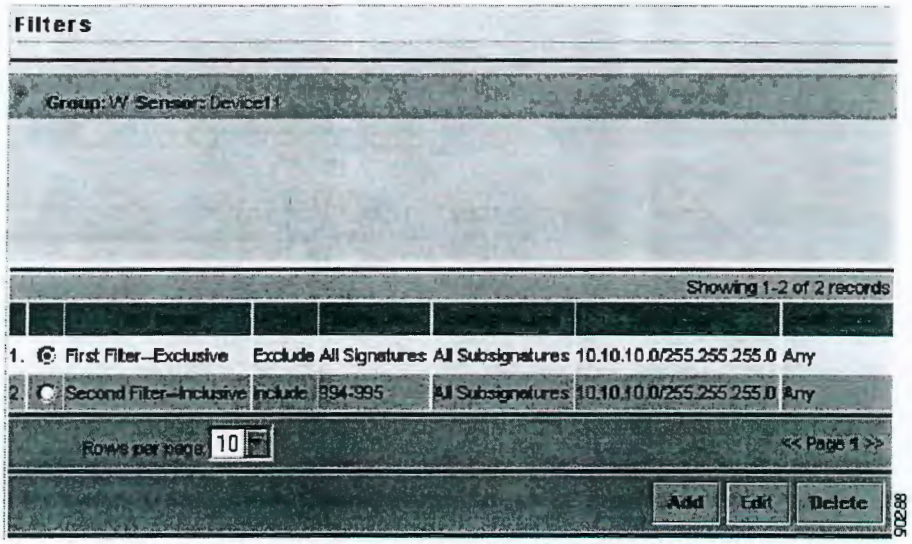


Step 22 To begin defining the inclusive filter in this example, click **Add**.

Step 23 Add a filter with the name "Second Filter--Inclusive" with an action of Include.

Step 24 Continue with this example by adding Signature 994 and Signature 995.

Step 25 Add the same source address and destination address that were used for the first filter, and then display the Filters page again. It should now appear as shown here.



The filter named `First Filter--Exclusive` will be applied first. It will exclude all alarms from Network 10.10.10.0. The filter named `Second Filter--Inclusive` will be applied next. It will allow alarms from Network 10.10.10.0 if they result from Signatures 994 or 995. Signatures 994 and 995 will not be disabled.

Specifying IP Fragment and TCP Session Reassembly Settings for a Sensor

The goal of defining these reassembly settings is to ensure that the sensor does not allocate all of its resources to datagrams that cannot be completely reconstructed, either because the sensor missed some frame transmissions or because an attack is generating random fragmented datagrams.

These settings ensure that valuable system resources are not reserved for sessions that are no longer active. These settings apply to sensors globally, not to individual settings such as signatures.

To specify IP fragment reassembly options and TCP session reassembly options, follow these steps:

Step 1 Select **Configuration > Settings**.

Step 2 In the TOC, click the **Object Selector** handle.

Step 3 In the Object Selector, select the sensor for which you want to specify reassembly options.

The Object Selector closes.

Step 4 In the TOC, select **Reassembly Options**.

The Reassembly Options page appears.

When configuring an IDSM or a 4.x sensor appliance, you have the option of TCP strict reassembly. The 3.x sensor appliance does not have that option.

When configuring a sensor appliance (3.x or 4.x), you have the option of specifying Maximum Total Fragments. The IDS module does not have that option.

Step 5 When configuring a 4.x sensor appliance, specify the operating system in the IP Reassemble Mode list box.

Step 6 To specify that you want the sensor to reassemble IP datagrams, select the **Reassemble Fragments** check box under IP Fragment Reassembly. Reassembling fragments is done by default by all sensors, both appliances and modules.

Step 7 To specify the maximum number of partial datagrams that the sensor can attempt to reconstruct at one time, enter that value in the Maximum Partial Datagrams field. Maximum Partial Datagrams is not available for 4.x sensor appliances.

Step 8 To specify the maximum number of fragments that can be accepted into a single datagram, enter that value in the Maximum Fragments Per Datagram field. Maximum Fragments Per Datagram is not available for 4.x sensors.

Step 9 To specify the maximum total fragments, enter that value in the Maximum Total Fragments field. Maximum Total Fragments is available for sensor appliances but not for IDS modules.

Step 10 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, enter that value in the Fragmented Datagram Timeout field.

Step 11 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 12 To specify how strict the reassembly requirements for this sensor should be when it attempts to reassemble the entire TCP session, select that type from the TCP Strict Reassembly list box. TCP Strict Reassembly is available for IDS modules but not for sensor appliances.

Step 13 To specify the number of seconds that can elapse before the sensor frees the resources allocated to a fully established TCP session, enter that value in the TCP Open Establish Timeout field.

Step 14 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, enter that value in the TCP Embryonic Timeout field.

Step 15 To accept your changes and close the Reassembly Options page, click **Apply**.

Tuning Your Sensor Configurations

After configuring your sensors, you must tune them to achieve optimal performance on your network, particularly to minimize false positives and false negatives.

Note Tuning sensor configurations should not be confused with tuning parameters for individual signatures.

To learn more, see Updating IDS Sensor Software Versions and Signature Release Levels, page 5-56.

Copying Configuration File Settings

You can copy configuration file settings from one sensor or sensor group to another sensor or sensor group.

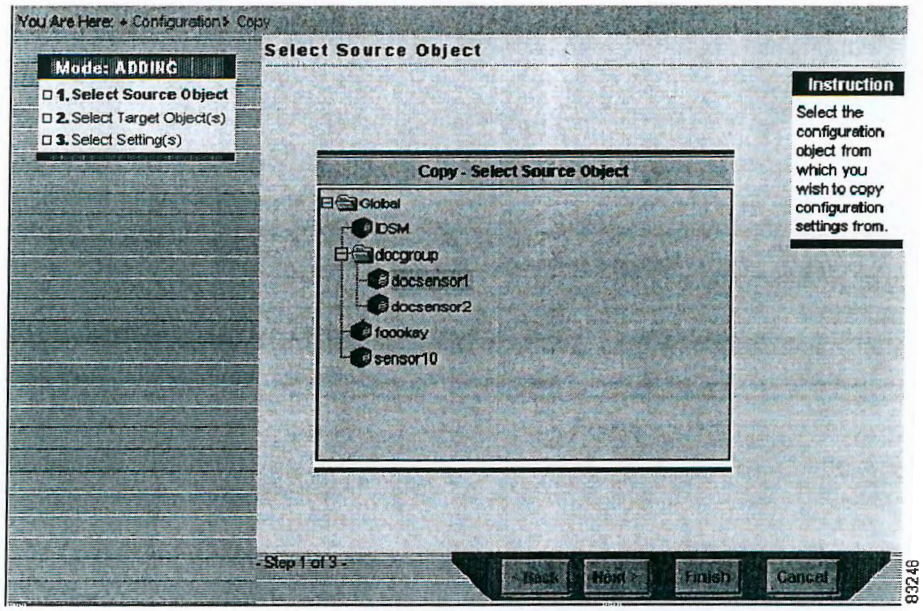
To copy configuration file settings, follow these steps:

Step 1 Select **Configuration > Copy**.

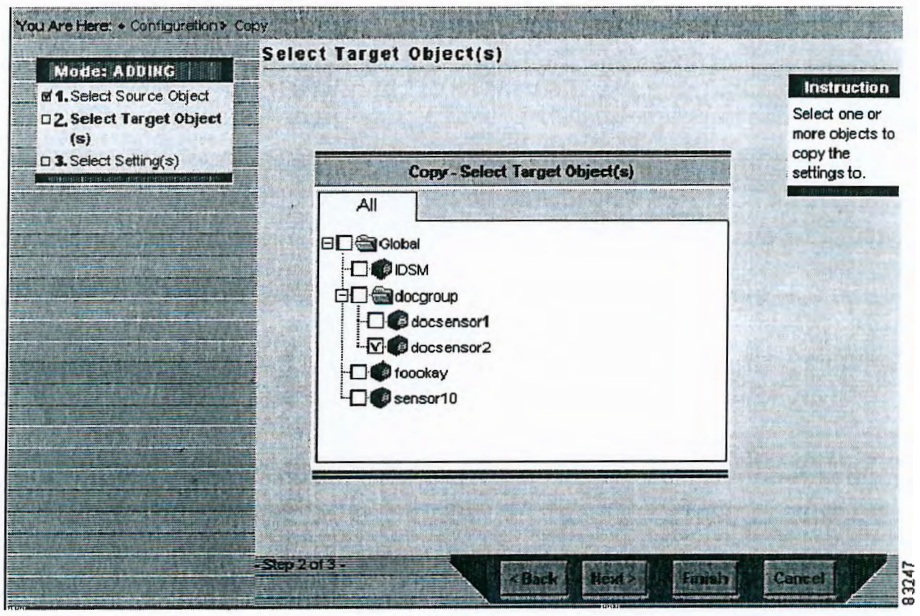
The first page of the Copy Wizard appears.

Step 2 Start the Copy Wizard. The Copy Wizard uses three steps to copy configuration file settings:

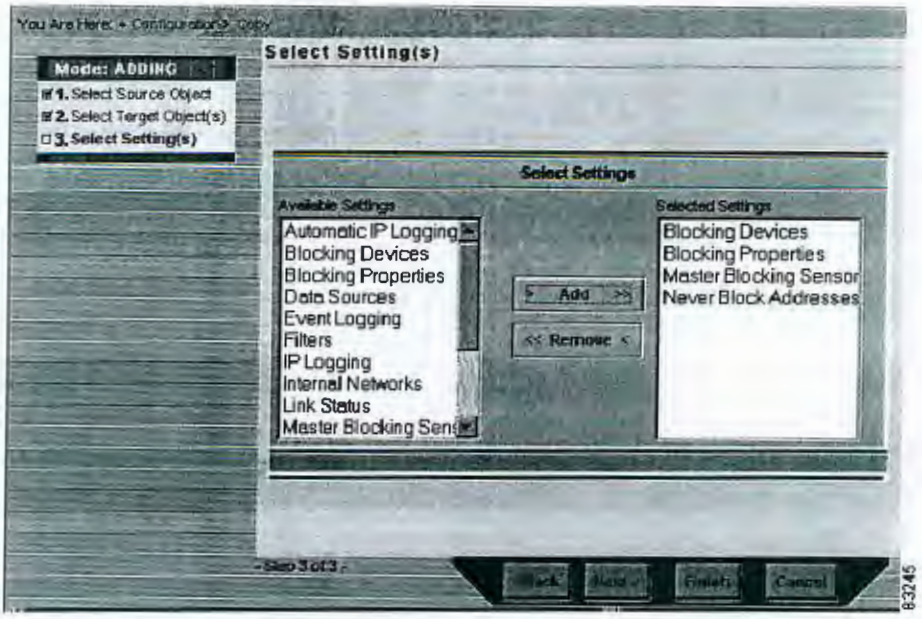
a. **Select Source Object.**



b. **Select Target Object(s).**



c. **Select Setting(s)**.



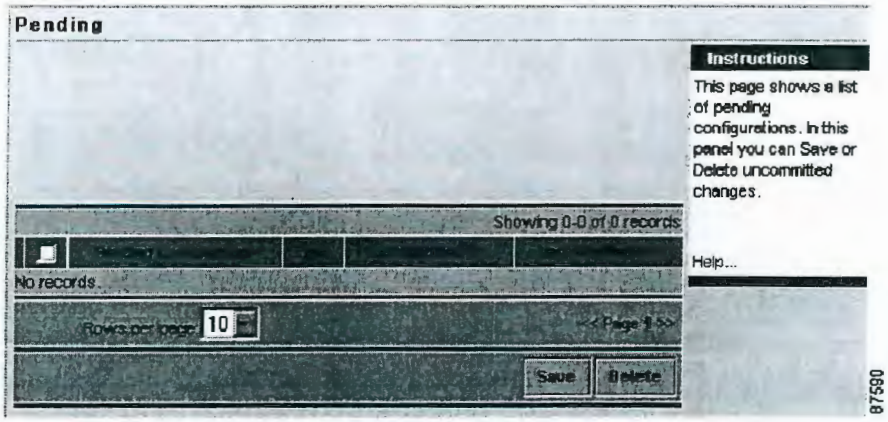
Reviewing Pending Configuration File Settings

You can review pending configuration file settings before committing them to the database. You also can delete settings if necessary.

To review pending configuration file settings, follow these steps:

Step 1 Select **Configuration > Pending**.

The Pending page appears.



Step 2 Select the check box associated with a sensor.

Step 3 Click **Save** to save the configuration; click **Delete** to delete it.

The Pending configuration page appears, no longer showing the pending configuration that you just saved or deleted.

Unlocking Pending Configuration Settings

A user who has pending configuration settings has a lock on those settings. No other users can commit those settings to the database or delete them. If a user has configuration settings that are pending, and the account of that user is deleted, you can use this procedure to take ownership of the pending settings. This procedure is also referred to as a "take lock" procedure because it can be thought of as "taking ownership" of or "unlocking" the settings.

This procedure illustrates the situation in which the account for doc-intern has been deleted, but a configuration is pending for the sensor named doc-intern-sensor.

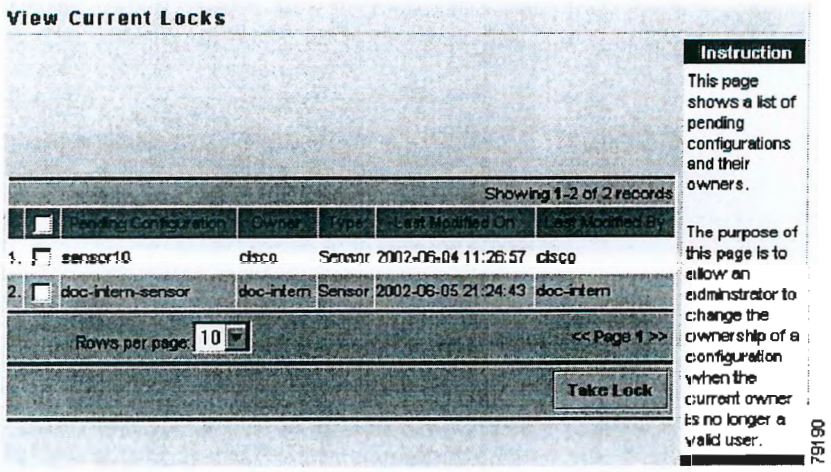
In this example, you are logged in as "admin" and you will take ownership of the pending configuration so that you can save it or delete it.

To unlock the pending configuration in this example, follow these steps:

Step 1 Select **Admin > System Configuration**.

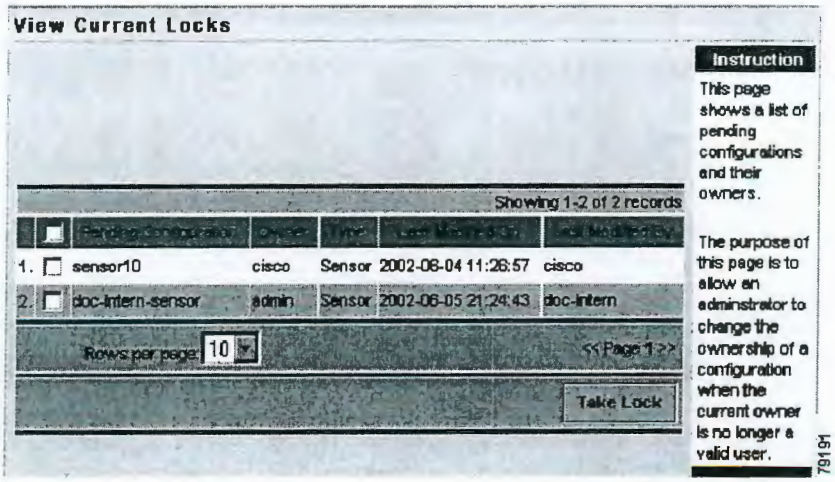
Step 2 In the TOC, select **View Current Locks**.

The View Current Locks page appears. Note that the owner of the pending configuration called `doc-intern-sensor` is `doc-intern`.



Step 3 Recall that in this example, you are logged in as "admin". Click **Take Lock**.

The View Current Locks page appears again. Now, note that you, logged in as `admin`, are the owner of the pending configuration.



Reviewing Historical Configuration File Settings

You can review historical configuration file settings for a sensor.

To review historical configuration file settings, follow these steps:

Step 1 Select **Configuration > Settings**.

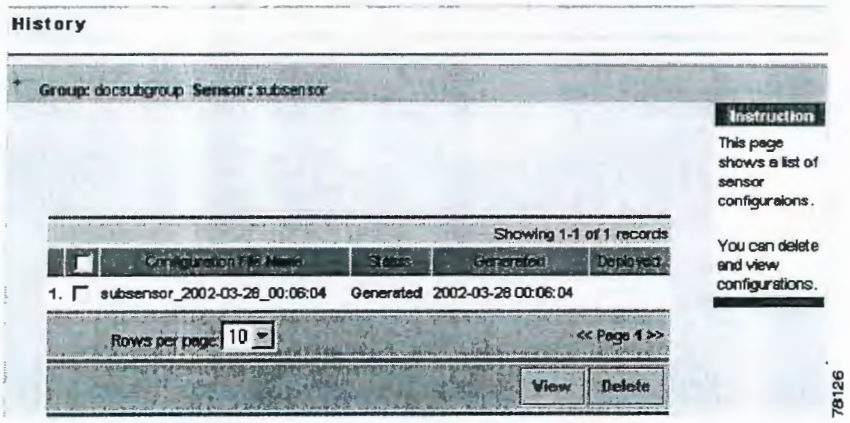
Step 2 In the TOC, click the **Object Selector** handle.

Step 3 In the Object Selector, select the sensor for which you want to review historical configuration file settings.

The Object Selector closes.

Step 4 Select **Configuration > History**.

The History page appears, and the Object bar displays the sensor you selected in the Object Selector.



Step 5 To view a configuration file, select the corresponding check box and click **View**.

Step 6 To delete a configuration file, select the corresponding check box and click **Delete**.

Updating IDS Sensor Software Versions and Signature Release Levels

Cisco Systems periodically releases updates of sensor software versions and signature release levels for its IDS Sensors (both sensor appliances and IDS modules). We recommend that you check for and perform regular updates of sensor software versions and signature release levels on sensors that you have deployed. This recommendation also applies to the server(s) where you have installed the IDS MC and Security Monitor.

Applicability: This procedure applies to Version 1.1 of the IDS MC and Version 1.1 of Security Monitor. When using the IDS MC, it can be used to update the server as well as any sensors that you select. When using Security Monitor, it can be used to update the server but not sensors; sensors are not (and cannot be) updated through Security Monitor.

Note We strongly recommend that you download and apply all update files, in order and without exception, as they become available. To be informed of the latest update files by e-mail, you can subscribe to the Cisco IDS Active Update Notification. The subscription form is available at http://www.cisco.com/warp/public/779/largeent/it/ids_news/subscribe.html.

Note We strongly discourage updating sensor software versions and signature release levels in a direct session to an individual sensor if you manage that sensor with the IDS MC. You should instead use this procedure of performing updates through the IDS MC. If you have changed the configuration of a sensor, or updated a sensor, outside of the IDS MC, we recommend that you delete that sensor from your configuration and then add it to your configuration.

Note Updating sensor software in a direct session to an individual sensor instead of by performing an update through the IDS MC will result in the rejection of the SSH fingerprint for that sensor. This is because the IDS MC is not involved in a session to an individual sensor.

To use this procedure effectively, you must understand the numbering system used for sensor software versions and signature release levels. For example:

- `3.1(2)S23`—A sensor appliance is operating with sensor software version 3.1, service pack 2, signature release level 23.
- `3.0(5)S20-IDSM`—An IDS module is operating with sensor software version 3.0, service pack 5, signature release level 20.

You should also understand the update files:

- Cisco releases its periodic updates of sensor software versions and signature release levels for its IDS Sensors in the form of update files that are compressed (.zip). IDS MC works with these compressed files directly; you should not extract anything from them.

- There are two types of update files:
  - **Service pack update files**—You can identify service pack update files by their names: the letters "sp" precede the version number. When these update files are applied, they change the version number of a sensor. Service pack update files contain executable code; they affect the actual micro-engine software on the sensor. They also contain signature updates.
  - **Signature update files**—Signature update file names contain the letters "sig" before the version number. Signature update files contain newly released signatures but not executable code.
- By inspecting the name of an update file, you can identify the device type (sensor appliance or IDSM), type of update (service pack or signature), version number, and signature release level. For example:
  - `IDSk9-sp-3.1-2-S23.zip`. This file has the following characteristics:
  - `IDSk9`—Applies to a sensor appliance.
  - `sp`—Contains a service pack update. Service pack updates include signature updates.
  - `3.1`—Applies to sensor software version 3.1.
  - `2`—Applies to Service Pack 2.
  - `S23`—Contains signature release level 23.
  - `zip`—Is compressed but should not be extracted.
  - `IDSM-sig-3.0-5-S20.zip`. This file has the following characteristics:
  - `IDSM`—This update file applies to an IDS module.
  - `sig`—Contains a signature update only.
  - `3.0`—Applies to sensor software version 3.0.
  - `5`—Applies to Service Pack 5.
  - `S20`—Contains signature release level 20.
  - `zip`—Is a compressed file but should not be extracted.

- The two types of update files are applied in different ways:
  - Service pack update files must be applied individually, stepwise, and sequentially. For example, if you are using a sensor appliance operating with `3.1(1)S32` and you want to update it to `3.1(3)S33`, you must apply the update file `IDSk9-sp-3.1-2-32.zip` and then the update file `IDSk9-sp-3.1-3-33.zip`.

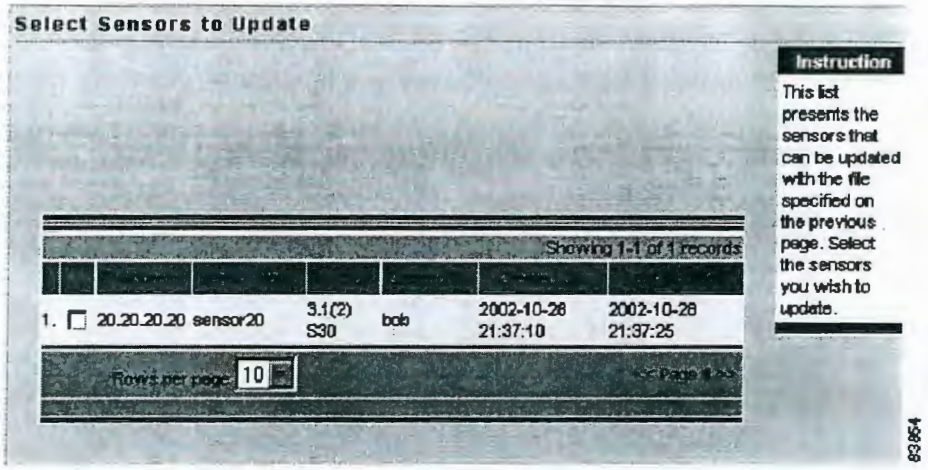
    Service pack update files can move major and minor version numbers. For instance, if you apply the first `3.1` service pack update to the last `3.0` version of a sensor, you will move the version number from `3.0` to `3.1`.
  - Signature update files do not need to be applied individually because they are cumulative. That is, a given revision level contains all the signatures from previous levels. For example, if you are using a sensor appliance operating with `3.1(3)S32` and you want to update it to `3.1(3)S34`, you can apply the update file `IDSk9-sig-3-1-S34.zip`.

    Signature update files can be applied only to sensors operating with the same version number, or with the same version number plus service pack designation. For example, the signature update file `IDSk9-sig-`**3.1-3-34**.zip can be applied to a sensor operating with version **3.1(3)**S32 but not to a sensor operating with version **3.1(2)**S22 or **3.1(4)**S34 or **3.0(3)**S22.

    Signature update files can be applied only to sensors that are not already operating at that file's signature revision level. For example, the signature update file `IDSk9-sig-3.1-3-`**34**.zip cannot be applied to a sensor operating with `3.1(3)` **S34**. The reason is that this sensor is already operating at the same signature version level (`S34`) that the update file provides.

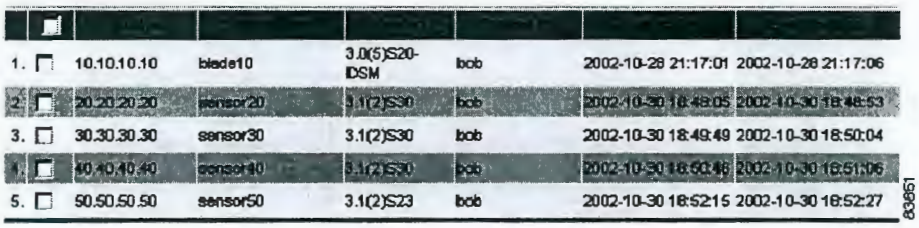
To use this procedure, you must have access to the server:

- You must have access to the IDS MC server if you want to update the IDS MC or a sensor.
- You must have access to the Security Monitor server if you want to update Security Monitor.
- If you have installed IDS MC and Security Monitor on the same server, you must have access to that server if you want to update the IDS MC or a sensor or Security Monitor.



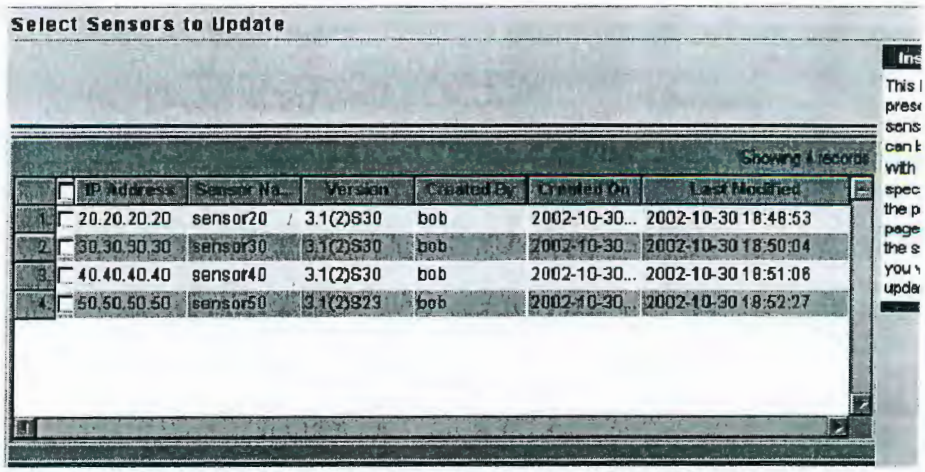
Do not select that sensor; instead, click **Cancel** and then continue this example with Step 10.

Step 10 Assume now that you have added three more sensors to your IDS MC installation, as illustrated here.



Select the same update file, `IDSk9-sp-3.1-3-S31.zip`, and then click **Apply**.

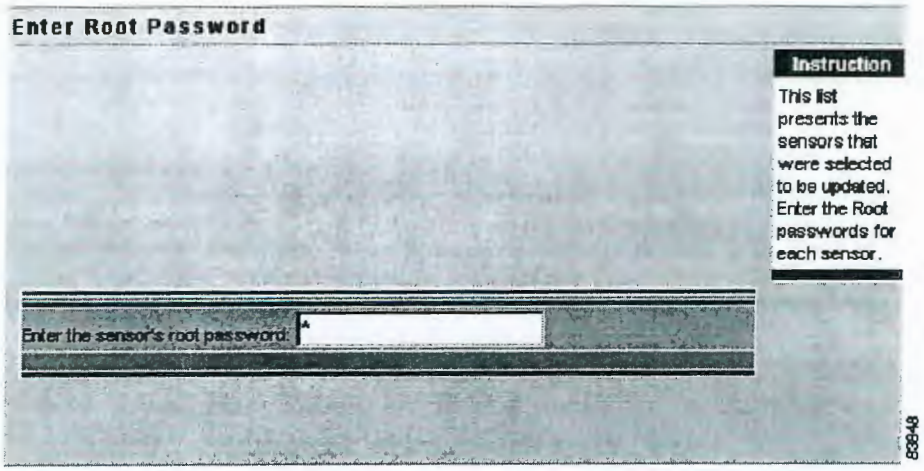
The Select Sensors to Update page appears as a scrolling table. There is no functional difference between the scrolling and non-scrolling forms of the Select Sensors to Update page. IDS MC 1.1 uses only the scrolling form of this table.



Recall that service pack update files must be applied individually, stepwise, and sequentially, as explained in the introduction to this procedure. Also recall that signature update files are cumulative. This means that the update file can be applied to all the sensors shown.

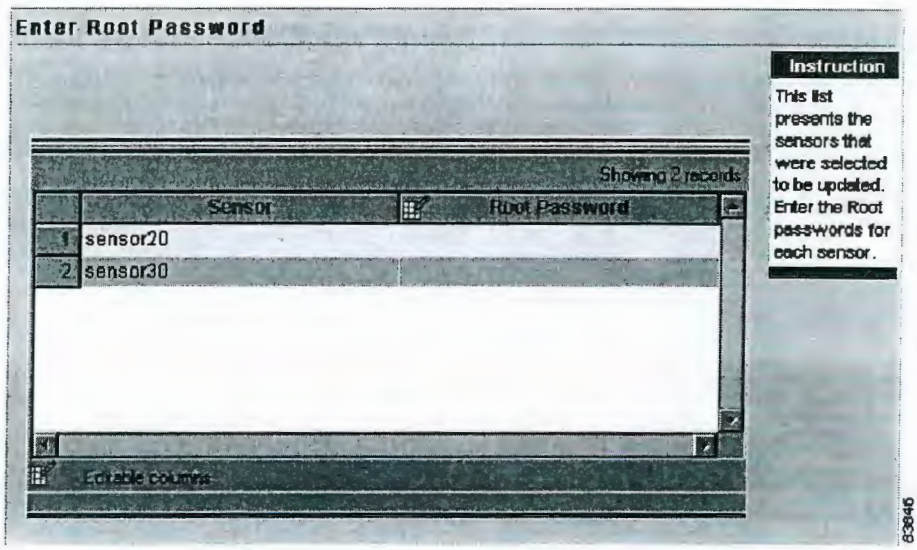
Step 11 As an example, select `sensor20`, and then click **Next**.

The Enter Root Password Page appears. In this example, only one sensor is being updated and IDS MC 1.0 is being used, so the Enter Root Password Page appears as a non-scrolling table. This non-scrolling table does not appear if IDS MC 1.1 is being used or if you are updating more than one sensor.

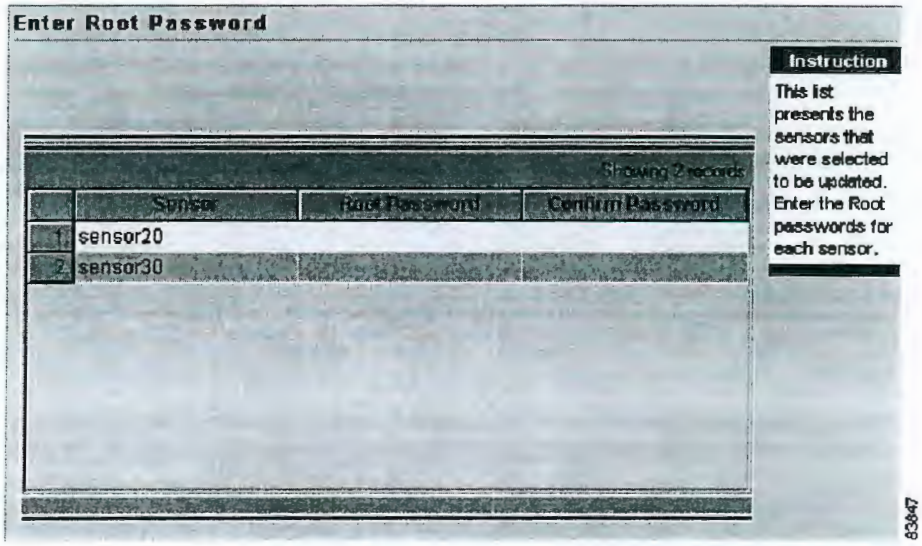


Note If the update file is an IDSM update file (not a sensor appliance update file), the Enter Root Password Page does not appear.

If you are using IDS MC 1.0 and you choose to update more than one sensor, `sensor20` and `sensor30`, for example, the Enter Root Password page appears as a scrolling table. There is no functional difference between these two forms of the Enter Root Password page.



IDS MC 1.1 uses a different form of this table.



Step 12 Enter the valid root password for each sensor. In IDS MC 1.1, enter the password a second time to confirm it.

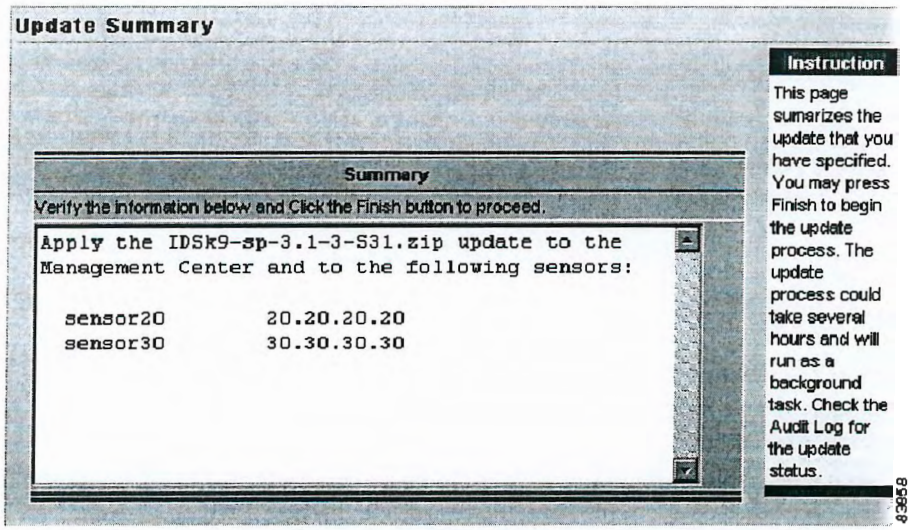
Note If you are using IDS MC 1.0, click outside the Root Password field after entering the last root password. This is required for your entry to be recognized as being completed. Clicking outside the Root Password field is not necessary in IDS MC 1.1.

Caution In IDS MC 1.0, when you enter root passwords in the scrolling table form of the Enter Root Password page, they will appear in clear text (unmasked). Do not allow your passwords to be observed while you are entering root passwords. Passwords are masked in IDS MC 1.1.

Tip When using sensor appliances (but not IDSMs), you can specify that root passwords be stored by IDS MC. To do so, select **Configuration > Settings**; from the TOC that appears, select **Identification**. On that page, you can specify that root passwords be persistent.

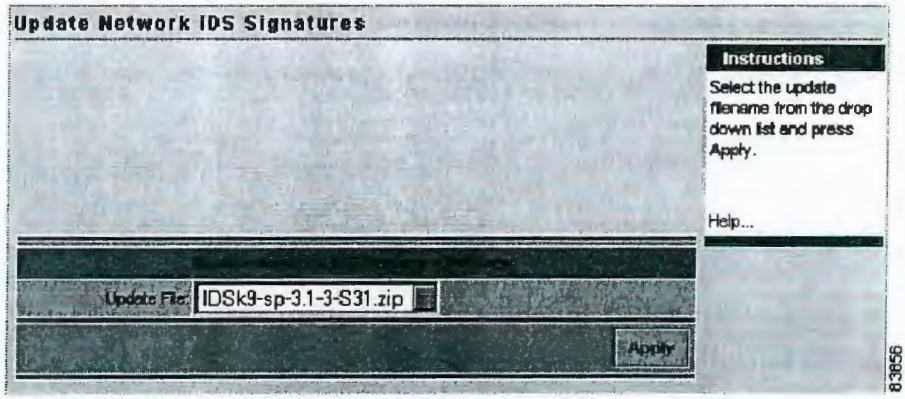
Click **Next**.

Step 13 The **Update Summary** page appears. This page describes the update that is about to be applied; in this example, an update is being applied to `sensor20` and `sensor30`.



Step 14 Click **Finish**.

The sensors you selected, if any, are updated using the update file that you chose in Step 8 or Step 9. In addition, the server where you installed IDS MC is updated. If you have installed Security Monitor on the server where you have installed IDS MC, this procedure will update the server operations that apply to Security Monitor; more specifically, this procedure will supply Security Monitor with the names of new signatures and an NSDB reference for them; sensors are not (and cannot be) updated through Security Monitor. The update process may take several minutes, depending upon the size and complexity of your network and its traffic. However, the update process is performed by a separate thread, so the Update Network IDS Signatures page appears again almost immediately.



Step 15 Verify that the update was successful by generating a report. The update process may take several minutes, depending upon the size and complexity of your network and its traffic.

a. Select **Reports > Generate**, and then click the **Audit Log Report** radio button.

b. Select **Select** to generate an audit log report. Use the audit log report to verify that you successfully updated your sensors and server using the update file that you downloaded from the Software Center.

Step 16 Verify that the update was successful by displaying a table of sensors in your installation. (The update process may take several minutes, depending upon the size and complexity of your network and its traffic.) For each group of sensors, select **Devices > Sensor**.

The Sensor page appears. Note that `sensor20` and `sensor30` were successfully updated to version `3.1(3)S31` by application of the update file `IDSk9-sp-3.1-3-S31.zip`

1.	☐	10.10.10.10	blade10	3.0(5)S20-IDSM	bob	2002-10-28 21:17:01	2002-10-28 21:17:06
2.	☐	40.40.40.40	sensor40	3.1(2)S30	bob	2002-10-30 16:50:46	2002-10-30 16:51:06
3.	☐	50.50.50.50	sensor50	3.1(2)S23	bob	2002-10-30 16:52:15	2002-10-30 16:52:27
4.	☐	20.20.20.20	sensor20	3.1(3)S31	bob	2002-10-30 19:09:11	2002-10-30 19:09:27
5.	☐	30.30.30.30	sensor30	3.1(3)S31	bob	2002-10-30 19:09:58	2002-10-30 19:10:17

83682

You should now return to Step 10 and update `sensor40` and `sensor50`. Then, skip Steps 17 through 25.

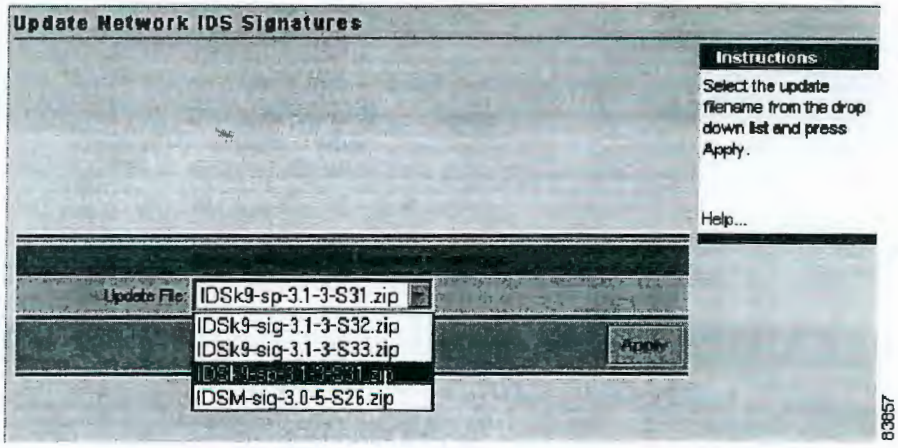
Note We strongly recommend that you download and apply all update files, in order and without exception, as they become available.

Step 17 To update your Security Monitor server only, complete Steps 17 through 21.

In Security Monitor, select **Admin > System Configuration**.

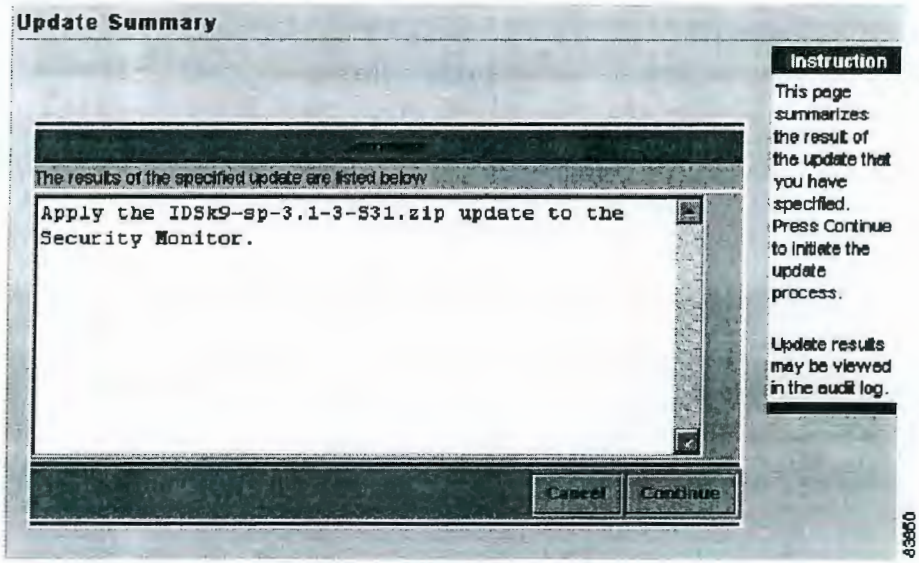
Step 18 From the TOC, select **Update Network IDS Signatures**.

The Update Network IDS Signatures page appears, showing all the update files, if any, that have been downloaded to `~CSCOpx/mdc/etc/ids/updates` on the server where you have installed Security Monitor.



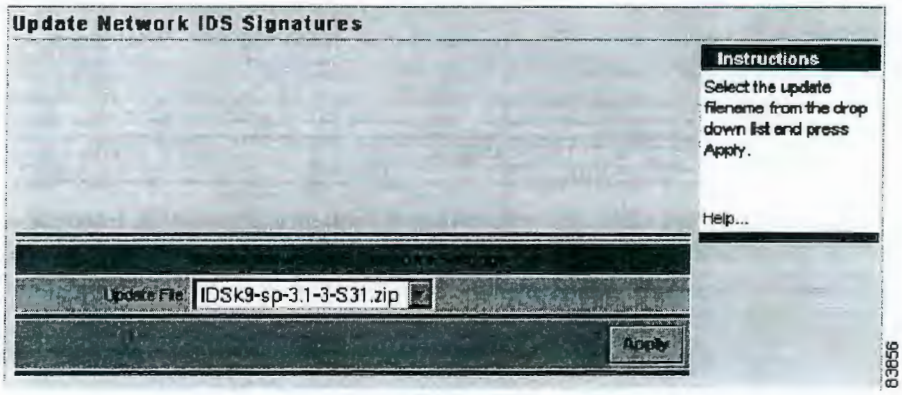
Step 19 Select an update file, `IDSk9-sp-3.1-3-S31.zip` in this example, from the Update File list, and then click **Apply**.

The Update Summary page appears. It states that the update file will be applied to Security Monitor.



Step 20 Click **Continue**.

The server where you installed Security Monitor is updated. The update process is performed by a separate thread, so the Update Network IDS Signatures page appears again almost immediately.



Step 21 Verify that the update was successful by generating a report.

a. Select **Reports > Generate**, and then click the **Audit Log Report** radio button.

b. Select **Select** to generate an audit log report. Use the audit log report to verify that you successfully updated your sensors and server using the update file that you downloaded from the Software Center.

Step 22 To update a sensor from sensor software 3.x to sensor software 4.x, complete Steps 22 through 25. Before you proceed with Step 22, you must gain physical access to the sensor and re-image it to sensor software 4.x. You must re-image it using a Cisco CD; you cannot download the software.

Note Some sensors cannot be re-imaged from 3.x to 4.x. Specifically, NRS platforms (the older Netranger sensors) cannot be re-imaged from 3.x to 4.x.

In IDS MC, select **Configuration > Updates**.

Step 23 From the TOC, select **Update Sensor Version**.

The Update Sensor Version page appears.

Step 24 Select the sensor that you want to update from a 3.x version to a 4.x version.

Step 25 Click **Update**.

The Update Status page appears.

Updating IDS Sensor Software from 3.x to 4.x

To update a sensor from sensor software 3.x to sensor software 4.x, you must have physical access to that sensor so that you can re-image it.

To update your sensor software from 3.x to 4.x, follow these steps:

Step 1 Gain physical access to the sensor and re-image it to sensor software 4.x. You must re-image it using a Cisco CD; you cannot download the software.

Note Some sensors cannot be re-imaged from 3.x to 4.x. Specifically, NRS platforms (the older Netranger sensors) cannot be re-imaged from 3.x to 4.x.

Select **Configuration > Updates**.

Step 2 From the TOC, select **Update Sensor Version**.

The Update Sensor Version page appears.

Step 3 Select the sensor that you want to update from a 3.x version to a 4.x version.

Step 4 Click **Update**.

The Update Status page appears.

VMS Bundle Component Installation

This chapter describes the system requirements and procedures for installing CiscoWorks Common Services, Management Center for PIX Firewalls (PIX MC), Management Center for IDS Sensors (IDS MC), and Monitoring Center for Security (Security Monitor). It also includes procedures to verify that you successfully installed the components.

System Requirements

CiscoWorks Common Services, PIX MC, IDS MC, and Security Monitor are components of the VPN/Security Management Solution (VMS).

You can install VMS CDs on Windows 2000. Table 2-1 shows VMS server requirements for Windows 2000 systems.

Table 2-1 Server Requirements

System Component	Requirement
Hardware	• IBM PC-compatible with a CD-ROM drive • Color monitor with video card capable of 16-bit colors
Processor	Pentium, 1 GHz, minimum

Table 2-1 Server Requirements (continued)

System Component	Requirement
Operating System	You must have one of the following operating systems: • Windows 2000 Server, Service Pack 2 or Service Pack 3 • Windows 2000 Professional, Service Pack 2 or Service Pack 3 **Note** CiscoWorks Common Services has not been tested with any other Windows or Windows 2000 operating system or service pack; therefore, installing CiscoWorks Common Services on any other operating system *is not supported.*
File System	NTFS
Memory	1 Gigabyte, minimum
Virtual Memory	2 Gigabytes, minimum
Hard Drive Space	9 Gigabytes of free hard drive space, minimum **Note** The actual amount of hard drive space required depends upon the number of CiscoWorks Common Services client applications you are installing and the number of devices you are managing with the client applications.

Additionally, you should not install CiscoWorks Common Services on a Windows server that is running any of the following services:

- Primary domain controller
- Backup domain controller
- Terminal server

You can access all product features from a client that fulfills the hardware, software, and browser requirements. Table 2-2 shows client hardware and software requirements.

Table 2-2 Client Hardware and Software Requirements

System Component	Requirement
Hardware/Software	IBM PC-compatible computer with 300 MHz or faster Pentium processor running one of the following: • Windows 98 • Windows NT 4.0 Workstation • Windows NT 4.0 Server • Windows 2000 Advanced Server • Windows 2000 Server or Professional Edition with Service Pack 2 or Service Pack 3 • Solaris SPARCstation or Sun Ultra 10 with a 333MHz processor running one of the following operating systems: – Solaris 2.7 – Solaris 2.8
Hard Drive Space	• 400 MB virtual memory (for Windows) • 512 MB swap space (for Solaris)
Memory	256 MB, minimum
Web Browser	You must also install one of the following HTML browsers: • Microsoft Internet Explorer 6.0 or 5.5 with Service Pack 2, and Java Virtual Machine (JVM) 5.00.3186 or later. **Note** PIX MC, Auto Update Server, and Router MC run only on Internet Explorer version 6.0 or 5.5 with Service Pack 2, and Java Virtual Machine (JVM) 5.00.3186 or later. • Netscape Navigator 4.79 (for Windows). • Netscape Navigator 4.76 (for Solaris).

Note CiscoWorks Common Services requires the Java Plugin from Sun Microsystems Java Runtime Environment (JRE) 1.3.1. CiscoWorks Common Services is not compatible with Java Plugin from JRE versions 1.2.x, 1.4.x, or any maintenance releases of JRE 1.3.1 (such as 1.3.1_01, 1.3.1_02, and so on). If the required JRE is not present on the client system, CiscoWorks Common Services downloads and installs it automatically; you do not need to install the JRE before accessing CiscoWorks Common Services. However, if an incompatible version of the JRE is present on the client system, you must remove it before accessing CiscoWorks Common Services. If you do not, some features of CiscoWorks Common Services may not function properly.

Installation Sequence

Complete the following tasks to install CiscoWorks Common Services, PIX MC, IDS MC, and/or Security Monitor.

Step 1 Bootstrap the managed devices.

Ensure that any supported devices you plan to manage, including PIX Firewalls and sensors, are installed on your network and that you can Telnet from the server to the managed device.

For more information, see Appendix A, "Network Device Preparation."

Step 2 Prepare the server and client systems.

Ensure that the server(s) on which you plan to install VMS components meet the minimum server system requirements. Additionally, ensure that any clients you will use to access the VMS components meet the minimum client system requirements.

For more information, see System Requirements, page 2-1.

Step 3 Install CiscoWorks Common Services.

Before you can install PIX MC, IDS MC, or Security Monitor, you must install CiscoWorks Common Services.

For more information, see Installing CiscoWorks Common Services as a Standalone Server, page 2-5.

Step 4 Install PIX MC.

PIX MC allows you to manage PIX Firewalls. You must install PIX MC on a server where CiscoWorks Common Services is installed.

For more information, see Installing PIX MC, page 2-11.

Step 5 Install IDS MC.

IDS MC allows you to manage IDS Sensors. You must install IDS MC on a server where CiscoWorks Common Services is installed.

For more information, see Installing IDS MC, page 2-12.

Step 6 Install Security Monitor.

Security Monitor allows you to collect, monitor, and view IDS Sensor postoffice events and PIX Firewall syslog messages. You must install Security Monitor on a server where CiscoWorks Common Services is installed.

Note For deployments in your production network and optimal performance, we recommend that you install Security Monitor on a server separate from the one running your Management Centers.

For more information, see Installing Security Monitor, page 2-14.

Step 7 Verify your installations.

Ensure that you successfully installed CiscoWorks Common Services, PIX MC, IDS MC, and Security Monitor.

For more information, see Verifying Your Installations, page 2-16.

Installing CiscoWorks Common Services as a Standalone Server

This section describes how to install CiscoWorks Common Services without first installing CiscoWorks. CiscoWorks Common Services contains the desktop and user authentication and authorization components found in CiscoWorks. However, you cannot run CiscoWorks applications, such as Resource Management Essentials, on a standalone installation of CiscoWorks Common Services.

Note For information about installing CiscoWorks Common Services on a server where CiscoWorks is already installed, see *Installing CiscoWorks Common Services 1.0 on Windows 2000*.

Before You Begin

- Obtain a license for CiscoWorks Common Services and make it available on the target server or floppy disk.
- Disable any virus scanning or intrusion detection software that may be running in the background on the server. These types of software can interfere with the installation.
- Close all other running programs.
- If you are reinstalling CiscoWorks Common Services, make sure the target directory is empty or does not exist before beginning the installation.

To install CiscoWorks Common Services in a standalone configuration, follow these steps:

Step 1 Put the Common Services 1.0 CD-ROM in the server CD-ROM drive, and then click **Install** on the Installer page that appears.

The CiscoWorks Common Services installation program starts. The Welcome page of the installation application appears.

If the installation program does not start, select **Start > Run** from the Windows taskbar, and then enter *d*`:/setup` in the Run dialog box, where *d* is the drive letter of the CD-ROM drive. Press **Enter** to start the installation program.

Step 2 Click **Next**.

The Software License Agreement page appears.

Step 3 To accept the terms of the license agreement, click **Yes**.

Note If you do not accept the terms of the license agreement, click **No**. The install wizard closes.

If you accepted the terms of the license agreement, the Choose Destination Location page appears. The default installation directory, `C:\Program Files\CSCOpx`, appears in the Destination Folder area.

Step 4 To change the default installation directory, click **Browse** and perform one of the following steps:

- Enter a new path in the Path field. If the directory specified does not exist, the installation program creates it.
- Use the Directories and Drives fields to navigate to an existing directory.

Step 5 Click **Next** to continue.

The System Requirements page appears.

Step 6 Review the requirements to ensure that the drive specified has enough free space for the installation. If the selected drive does not have enough free space, perform one of the following steps:

- Click **Back** to return to the Choose Destination Location screen and select a drive that meets the drive space requirements.
- Click **Cancel** to terminate the installation. You need to either install additional drive space on the target system or install CiscoWorks Common Services on a system that has the drive space requirements.

Verify that the system has enough memory. If the system does not have enough memory, click **Cancel** to terminate the installation. You should either install additional memory in the target system or install CiscoWorks Common Services on a system that meets the minimum memory requirements.

If your system meets all of the system requirements, click **Next**.

The Select License File screen appears.

Step 7 Enter the path to the license file in the License file location field. You can also use the Browse button to navigate to the correct license file. Click **Next** to continue.

Note You can bypass this step by clicking **Skip**. However, some of the client applications will not function if you do not enter a valid license. Refer to your client application documentation to note the licensing requirements for the applications you plan to install.

The Account Information page appears.

Step 8 Enter the password used to log in to Windows in the Password and Confirm Password fields. Click **Next** to continue.

If the two passwords do not match, the system prompts you to enter them again. If the passwords match, the Ports Configuration page appears.

Step 9 To change the external port numbers used by the Lock Manager (lm.exe) and database (fms.exe) services, enter the new information in the following fields:

- **LM Port**—The port used by Lock Manager. The default value is 1272. Use the default value unless it conflicts with another application on the server.
- **FMS Port**—The port used by the CiscoWorks Common Services database. The default value is 9652. Use the default value unless it conflicts with another application on the server.

Click **Next** to continue.

The Database Configuration page appears.

Step 10 Enter the information used by the SQL database component of CiscoWorks Common Services:

- **Server Port**—The port used by the SQL database. The default value is 10033. Use the default value unless it conflicts with another application on the server.
- **Password**—The password used by the SQL database. The password must be at least 4 characters long.
- **Confirm Password**—The same value you entered in the Password field.

Click **Next** to continue.

The Apache Server Configuration page appears.

Step 11 Enter the information used by the Apache server component of CiscoWorks Common Services:

- **HTTPS Port**—The port used by Apache for Secure Socket Layer (SSL) requests. Use the default value, 443, unless it conflicts with another application on the server.
- **Email Address**—The e-mail address of the system administrator (required).
- **SMTP Server**—The DNS name or IP address of your SMTP server.

Click **Next** to continue.

The Certificate Generation page displays.

Step 12 Enter the following information required to generate the local certificate. The local certificate is used for authentication and authorization when you login to the CiscoWorks desktop:

- **Country Code**—A two-character code for the country where the CiscoWorks Common Services server is located.
- **State**—The name of the state or province where the CiscoWorks Common Services server is located.
- **City**—The name of the city where the CiscoWorks Common Services server is located.
- **Company**—Your company name.
- **Organization**—The name of the organization or division you work in.
- **Domain**—The name of the domain the server resides in.
- **Certificate Password**—A password for the certificate. The password must have a minimum of 4 and a maximum of 10 alphanumeric characters.
- **Confirm Password**—The same value you entered in the Certificate Password field.

Note You cannot leave any of the fields blank. If one of the above fields does not apply to you, enter any text of your choosing in the field.

Click **Next** to continue.

The Create Shortcuts page appears.

Step 13 To create a shortcut on the Windows desktop, select the **Create a shortcut...** check box, and then click **Next** to continue.

The Verification page appears.

Step 14 Review your settings. If you need to change any settings, click **Back** to return to the setting you need to change. Click **Next** to continue.

The Start Copying Files page appears. During the file copy, the system prompts you four different times to change passwords for the following components:

- The casuser account (the user created by CiscoWorks Common Services to run the desktop services)
- The "admin" account

- The "guest" account
- The CMF database

Note If you abort the installation during the file copy stage, you must run the uninstall program before you attempt to install CiscoWorks Common Services again.

Step 15 To accept the default passwords, click **No**.

Note The default password for the admin account is "admin". The default password for the "guest" account is none (blank). You can change these passwords at a later time. The default passwords for causer and the database are generated by the system; you cannot change them later.

To change a password, follow these steps:

a. Click **Yes**.

b. Enter the password in the Password field.

c. Re-enter the password in the Confirm field.

d. Click **OK**.

The installation may take a few minutes to complete while the components are installed and the services are configured. When the installation is complete, the Restart page appears.

Step 16 Select **Yes** and click **Finish** to restart the computer. Select **No** and click **Finish** to restart the computer at a later time.

Note You must restart the computer before you use CiscoWorks Common Services.

Installing PIX MC

This section describes how to install PIX MC. This procedure assumes that you have already installed CiscoWorks Common Services.

To install PIX MC, follow these steps:

Step 1 Log in as the local administrator on the system on which you installed CiscoWorks Common Services.

This user account *must* be the same one used to install CiscoWorks Common Services.

Step 2 Insert the PIX MC CD into the CD-ROM drive, and then click **Install** on the Installer page that appears.

If the installation program does not start, select **Start > Run** from the Windows taskbar, and then enter *d*:/setup in the Run dialog box, where *d* is the drive letter of the CD-ROM drive. Press **Enter** to start the installation program.

The Welcome page appears.

Step 3 Click **Next**.

The Software License Agreement page appears.

Step 4 To accept the terms of the license agreement, click **Yes**.

Note If you do not accept the terms of the license agreement, click **No**. The install wizard closes.

The System Requirements page lists the details of your available system resources compared with the requirements of PIX MC.

Caution If your system does not meet the system requirements, we recommend that you exit the installation and see your system administrator for assistance installing the application.

Step 5 Click **Next**.

The Verification page lists the details of the installation and asks you to confirm that you want to proceed.

Step 6 Click **Next**.

Installation progress is displayed while files are copied and tools are configured. PIX MC is installed by default in the same location where CiscoWorks Common Services is installed. That default location is `C:\Program files\CSCOpx`. When the installation is complete, the Setup Complete page appears.

Step 7 Click **Finish**.

Installing IDS MC

This section describes how to install IDS MC.

This procedure assumes that you have already installed CiscoWorks Common Services.

Tip For enhanced performance, we recommend that you install IDS MC and Security Monitor on separate servers. If you are installing IDS MC and Security Monitor on the same server, follow the installation procedure in *Installing Management Center for IDS Sensors 1.0 and Monitoring Center for Security 1.0 on Windows 2000*.

To install IDS MC, follow these steps:

Step 1 Log in as the local administrator on the system on which you installed CiscoWorks Common Services.

Step 2 Insert the Monitoring Center for Security and Management Center for IDS Sensors CD into the CD-ROM drive, and then click **Install** on the Installer page that appears.

If the installation program does not start, select **Start > Run** from the Windows taskbar, and then enter *d*:/setup in the Run dialog box, where *d* is the drive letter of the CD-ROM drive. Press **Enter** to start the installation program.

The Welcome page appears.

Step 3 Click **Next** to begin the installation.

The Software License Agreement page appears.

Step 4 To accept the terms of the license agreement, click **Yes**.

Note If you do not accept the terms of the license agreement click **No**. The install wizard closes.

Step 5 Select the **Custom installation** radio button. Then, click **Next**.

Step 6 To install IDS MC, select the **IDS MC only** radio button. Then, click **Next**.

The System Requirements page appears.

Step 7 Verify that your system meets the minimum disk space and memory requirements. Then, click **Next**.

The Verification page appears.

Step 8 Verify the selected components. Then, click **Next**.

The Select Database Location page appears.

Step 9 By default, the database is located in the directory where CiscoWorks Common Services is installed. To specify a different directory for the IDS database, enter a file path in the Database file location field. Then, click **Next**.

The Select Database Password page appears.

Step 10 Enter the database password in the **Password** field. Then, to confirm the password, reenter it in the **Confirm Password** field. Then, click **Next**.

The Restart page appears.

Step 11 Select **Yes, I want to restart my computer now** and click **Finish** to restart the computer. Select **No, I will restart my computer later** and click **Finish** to restart the computer at a later time.

Note You must restart the computer before you use IDS MC.

Installing Security Monitor

This section describes how to install Security Monitor.

This procedure assumes that you have already installed CiscoWorks Common Services.

Tip For enhanced performance, we recommend that you install IDS MC and Security Monitor on separate servers. If you are installing IDS MC and Security Monitor on the same server, follow the installation procedure in *Installing Management Center for IDS Sensors 1.0 and Monitoring Center for Security 1.0 on Windows 2000*.

To install Security Monitor, follow these steps:

Step 1 Log in as the local administrator on the system on which you installed CiscoWorks Common Services.

Step 2 Insert the Monitoring Center for Security and Management Center for IDS Sensors disc into the CD-ROM drive, and then click **Install** on the Installer page that appears.

If the installation program does not start, select **Start > Run** from the Windows taskbar, and then enter *d*:/setup in the Run dialog box, where *d* is the drive letter of the CD-ROM drive. Press **Enter** to start the installation program.

The Welcome page appears.

Step 3 Click **Next** to begin the installation.

The Software License Agreement page appears.

Step 4 To accept the terms of the license agreement, click **Yes**.

Note If you do not accept the terms of the license agreement click **No**. The install wizard closes.

Step 5 Select the **Custom installation** radio button. Then, click **Next**.

Step 6 To install Security Monitor, select the **Security Monitor only** radio button. Then, click **Next**.

The System Requirements page appears.

Step 7 Verify that your system meets the minimum disk space and memory requirements. Then, click **Next**.

The Verification page appears.

Step 8 Verify the selected components. Then, click **Next**.

The Select Database Location page appears.

Step 9 By default, the database is located in the directory where CiscoWorks Common Services is installed. To specify a different directory for the IDS database, enter a file path in the Database file location field. Then, click **Next**.

The Select Database Password page appears.

Step 10 Enter the database password in the **Password** field. To confirm the password, reenter it in the **Confirm Password** field. Then, click **Next**.

The Select CW2000 Syslog Port page appears.

Step 11 Specify which UDP port CiscoWorks uses. The value can be between 1 and 65,535. By default, CiscoWorks uses UDP port 52514. We recommend that you use the default port value. Then, click **Next**.

The Configure Communication Properties page appears.

Step 12 To submit the communication properties for this host, enter the appropriate values in the Host ID, Organization ID, IP Address, Host Name, and Organization Name fields. Then, click **Next**.

The properties are used to establish the communication infrastructure for this host and the IDS sensor. The Restart page appears.

Step 13 Select **Yes, I want to restart my computer now** and click **Finish** to restart the computer. Select **No, I will restart my computer later** and click **Finish** to restart the computer at a later time.

Note You must restart the computer before you use Security Monitor.

Verifying Your Installations

This section describes how to log in to CiscoWorks and how to verify installation of CiscoWorks Common Services, PIX MC, Security Monitor, and Security Monitor. It contains the following sections:

Verifying the CiscoWorks Common Services Installation

You can verify the success of the installation before you log in to CiscoWorks Common Services.

To verify the CiscoWorks Common Services installation, follow these steps:

Step 1 Open a DOS prompt, enter **net start**, and press **Enter**.

A list of Windows 2000 services appears.

Step 2 Verify that the following services are running:

- Apache WebServer
- CMF rsh/rcp service
- CMF syslog service
- CMF tftp service
- CW2000 Daemon Manager
- CW2000 Device Agent Framework
- CW2000 KRS Database
- CW2000 Lock Manager
- CW2000 Sybase Server
- CW2000 Tomcat Servlet Engine
- CW2000 Web Server
- JRun Proxy Server for CW2000

If any of these services is not present, reboot the system to start the services. If the missing services do not appear after rebooting the server, the installation was unsuccessful.

Logging in to CiscoWorks2000

The CiscoWorks2000 Server desktop is the interface for the CiscoWorks network management applications, including Security Monitor, IDS MC, and PIX MC. The desktop is a graphical user interface that runs in a browser. For additional information about the CiscoWorks2000 Server desktop, see *Getting Started with the CiscoWorks2000 Server Desktop*.

Before you log in, make sure that your browser is configured correctly for CiscoWorks. For more information, see *Installing CiscoWorks Common Services 1.0 on Windows 2000*.

If you have installed CiscoWorks and are logging in for the first time, you can use the reserved "admin" username and password.

To log in to CiscoWorks, follow these steps:

Step 1 Access the CiscoWorks2000 Server from your web browser.

Step 2 Enter **admin** in both the Name and Password fields of the Login Manager.

Note If you changed the default password for the **admin** account during the install, use that new password. If you did not change the default password when you installed CiscoWorks Common Services, we strongly recommend that you perform Step 4 to change it.

Step 3 Click **Connect** or press **Enter**. You are now logged in.

Step 4 Select **Server Configuration > Setup > Security > Modify My Profile** to change the admin password.

Verifying Installation by Checking Package Options

You can verify the installation of PIX MC, IDS MC, and Security Monitor in the Packages Installed section of the About the Server page from the CiscoWorks2000 desktop.

To verify installation from the About the Server page, follow these steps:

Step 1 Select **Server Configuration > About the Server > Applications and Versions**.

The About the Server page appears.

Step 2 Verify that IDS MC and Security Monitor are listed in the Applications Installed list of the About the Server page and that Management Center for PIX Firewalls is listed in the Packages Installed list.

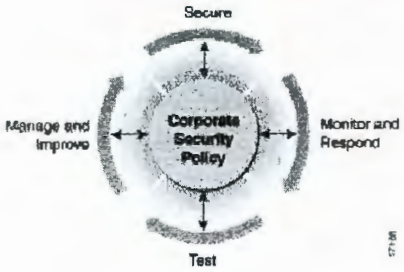
Managing Sensors with IDS MC

This chapter outlines the task flow that you need to follow to manage your sensors with Management Center for IDS Sensors (IDS MC). First, however, you must develop a security policy that enables the application of security measures. Your security policy should:

- Identify security objectives for your organization.
- Document the resources you want to protect.
- Identify the network infrastructure with current maps and inventories.
- Identify the critical resources (such as research and development, finance, and human resources) that you want to give extra protection to.

When you have developed your security policy, it becomes the hub of the Cisco Security Wheel, shown in Figure 3-1.

Figure 3-1 Cisco Security Wheel



The spokes of the Cisco Security Wheel represent network security as a continual process consisting of the following four steps:

1. Secure your system.
2. Monitor the network for violations and attacks against your security policy and respond to them.
3. Test the effectiveness of the security safeguards in place.
4. Manage and improve corporate security.

You should continually perform all four steps, and you should consider each of them when you create and update your corporate security policy.

IDS MC is management software for Cisco Intrusion Detection System. Cisco Intrusion Detection System provides real-time monitoring of network traffic for suspicious activities and active network attacks. The network devices that monitor network traffic are called sensors. Sensors are similar to multihomed hosts in that often they are connected to two physically different networks. However, they are unlike multihomed hosts in that only one connection is addressable. In other words, the adapter that is connected to the monitored network(s) is not addressable—it runs as a promiscuous adapter, studying each network packet that it senses on the physical medium. Sensors come in two physical models: dedicated, standalone network appliances and line card modules running in certain Cisco Catalyst 6000 switches.

The sensor compares network packets to its signatures to determine if the contents of the network packets meet the criteria of an attack. A *signature* is a pattern of traffic, often thought of as a set of rules, that your sensor uses to detect typical intrusive activity, such as denial of service (DoS) attacks. When the packets match a given signature rule, an alarm is generated and sent to Security Monitor.

Note Some signatures monitor for normal network activity, rather than for an attack. For example, Signature 2004, ICMP Echo Request, may result in a large number of alarms generated not by attacks, but by normal network traffic.

You can configure a sensor to issue commands to a Cisco router to block any packets from the source IP address that triggers an alarm for specific signatures. These commands are issued as temporary changes to the access control list (ACL) of the Cisco router. After a specified period of time, the sensor removes those

commands, restoring the router to its pre-attack configuration state. The sensor can also make similar changes to the Cisco PIX Firewall and the Cisco Catalyst 6000 switch.

Sensors have a number of settings associated with them, beginning with the following:

- The IP address that IDS MC uses to communicate with the sensor.
- The software version that is running on the sensor.
- The signatures that are used to study network traffic.
- The signature overrides that may have been applied.
- The devices that are used to block active attacks.
- The networks and syslog data streams that are monitored.
- Whether the sensor copies its alarm log data to an FTP server.

The sensor follows a basic task flow from initial setup to deployment. The following list identifies the primary tasks and the order in which you should perform them.

1. Bootstrap the sensor so that IDS MC can detect the sensor on the network. Bootstrapping involves getting the sensor up and running on the network, assigning it an IP address, and connecting it to the physical media.
2. Add the sensor to IDS MC. Next, manually define the settings that match the configuration settings of the bootstrapped sensor.
3. Configure signatures for specific responses to an attack, such as logging the packets to and from the source address of an alarm, to a file. You can edit an existing signature or define a new signature.
4. Tune the signatures for the sensor. You can tune sensor signatures using four general methods: by specifying reassembly options for IP fragments and TCP sessions, by identifying hosts and networks that should be exempt from sending an alarm for certain signatures, by filtering alarms in accordance with their severity, and by changing parameters for the signature (such as identifying which ports to monitor).
5. Generate, approve, and deploy the configuration files to the sensors.
6. Use Security Monitor to view historical and real-time attack and system status notifications. After you configure the sensors to study network activities, any notifications generated by the sensors are published to the database. Using Security Monitor, you can study these notifications to

determine what attacks are ongoing and to gather status information about the sensors, such as which ones have generated blocking rules for detected attacks.

Placing a Sensor on Your Network

This section discusses the best way to deploy and configure sensors on your network. It has the following topics:

Deciding Where to Place Sensors in Your Network

Deciding where to place sensors in your network means that you must carefully examine the connections between your network and other networks, including the Internet. In the process, you will also need to study the size and complexity of your network and the amount and type of traffic on your network.

Studying these characteristics of your network will also help you determine the number of sensors required and the hardware configuration for each sensor (for example, the size and type of network interface cards). IDS MC is designed to support at least 300 sensor deployments.

Note Refer to the *Intrusion Detection Planning Guide* for detailed information about intrusion detection deployment: http://www.cisco.com/univercd/cc/td/doc/product/iaabu/idpg/index.htm

The sensor monitors all traffic crossing a given network segment. Keeping that in mind, consider all the network connections you want to protect. These connections fall into four basic categories, or locations, as illustrated in Figure 3-2 and described in the following paragraphs.

Figure 3-2 Major Types of Network Connections

In location 1, the sensor is placed to monitor traffic between the protected network and the Internet. This is commonly referred to as *perimeter protection* and is the most common deployment for a sensor. This location can be shared with firewall protection, and is discussed in Placing a Sensor on Your Network, page 3-7.

In location 2, the sensor is monitoring an extranet connection with a business partner. Although most organizations have defined policies on the use and security of this type of connection, there is no guarantee that the partner network is adequately protected. Consequently, an outsider can enter your network through this type of connection. These extranet connections also may have firewalls.

In location 3, the sensor is monitoring the network side of a remote access server, labeled Dial-up server in Figure 3-2. Although this connection may be for employee use only, it could be vulnerable to external attack.

In location 4, the sensor is monitoring an intranet connection. For example, the protected network of one department may contain an e-commerce site where all the connection types described so far are required. The network of another department may contain company-specific research and development or other engineering information and should be given additional protection.

Keeping these connection types in mind, consider the network you want to protect. Determine which segments to monitor. Remember that each sensor maintains signatures configured for the segment it monitors. Signatures can be standard across the organization or unique for each sensor. You may consider defining your network topology to force traffic across a specific monitored network segment. There are always operational trade-offs when determining sensor placement. The end result should be a good idea of where to place sensors in your network, the number of them, and their hardware configuration.

How the Sensor Functions

The next step in protecting your network is understanding how the sensor captures network traffic.

Each sensor comes with two interfaces. In a typical installation, one interface monitors the desired network segment, and the other interface communicates with the IDS MC and other network devices. The *monitoring interface* operates in promiscuous mode, meaning it has no IP address and is not visible on the monitored segment.

The sensor captures network traffic at the IP layer. Therefore, it must understand and interpret Media Access Control (MAC) layer protocols, which most networks use to pass along data packets.

The *command and control interface* is always an Ethernet interface. This interface has an assigned IP address, which allows it to communicate with IDS MC or other network devices (typically Cisco routers). Although this interface is "hardened" from a security perspective, it is visible on the network and must be protected.

When responding to attacks, the sensor can do the following:

- Insert TCP resets via the monitoring interface.

Note The TCP reset action is only appropriate as an action selection on those signatures associated with a TCP-based service. If selected as an action on non-TCP-based services, no action is taken. Additionally, TCP resets are not guaranteed to tear down an offending session because of limitations in the TCP protocol.

- Make ACL changes to block traffic on routers (or PIX Firewall or Cisco Catalyst 6000 switches) that the sensor manages, using the command and control interface.

Note Such routers are referred to as *blocking routers*, and the sensor opens and maintains a Telnet session (or an SSH session, in the case of a PIX Firewall) to such routers to reduce the time required to publish the ACL rule sets that block traffic.

The last step in understanding how a sensor functions is the data speed or load on the monitored network. Because the sensor is not in the data path, it has no impact on network performance. However, there are limitations on the data speeds it can monitor. The following list identifies the available models and the maximum network speed they can monitor:

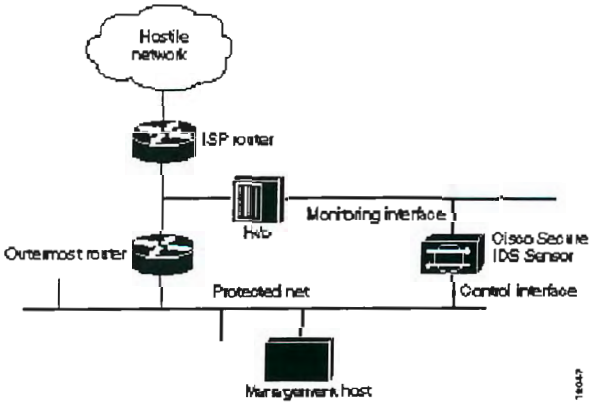
- IDS 4230 sensor appliance—Supports up to 100 Mbps.
- IDS 4210 sensor appliance—Supports up to 45 Mbps.
- Intrusion Detection Module for Catalyst 6000—Supports up to 120 Mbps, depending on network traffic.

Placing a Sensor on Your Network

You can place a sensor in front of or behind a filtering router. Each position has benefits and drawbacks.

Placing the monitoring interface of the sensor in front of a filtering router allows the sensor to monitor all incoming and outgoing network traffic. However, when deployed in this manner, the sensor cannot normally detect internal network traffic. An internal attacker taking advantage of vulnerabilities in network services would remain undetected by the external sensor (see Figure 3-3). In Figure 3-3, the Outermost router is the filtering router.

Figure 3-3 Sensor in Front of a Filtering Router



Placing the monitoring interface of the sensor behind a filtering router shields the sensor from any attacks that the filtering router blocks. This configuration provides a more robust reaction capability because the sensor can work with the router to block future attacks.

Deployment Considerations

To enable the sensor to manage the filtering router to defend your network, you must do the following:

- Enable Telnet services on the router.
- Add the router to the Object Selector in IDS MC.

The sensor then will be able to dynamically update the router ACLs to deny unauthorized activity.

ICMP Reply Flood

General Affected External

General

Key Attributes

Attributes/Severity	**Medium Severity**
Vulnerability Type:	Network
Exploit Type:	Denial

Description
This attack uses broadcast addresses to multiply a spoofed packet stream and direct it at a target host.

First, a series of spoofed ICMP Requests (Echo, Timestamp, or Address Mask) packets claiming to be from a victim machine are sent to a broadcast address. When such a packet arrives at the destination network, ALL machines will respond with a reply to the spoofed address. This generates many responses for each request, in effect multiplying the initial stream by one or more orders of magnitude. When all these responses arrive at the target machine, they can clog or crash it. This can also affect the routers tasked with relaying all these packets. The broadcast address can be either inside or outside the victim's network.

Consequences
An attacker can tie up some or all of a network's bandwidth.

Countermeasures
To prevent your routers from being used as intermediaries in this attack, turn off directed broadcasts on all your internal and external routers. To avoid being the victim, you need to set your perimeter routers to reject incoming ICMP reply packets. This will prevent any internal machines that are protected from pinging outside machines.

Access
Access Required: network access
Access Gained:

Products
IDS Signature Smurf

SignatureId/ SubId	2153/0
CSID Versions:	2.1.1
Signature Description	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. Since 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.
Alarm Level	4

Benign Triggers	Network administration tools that send out broadcast ICMP Requests could trigger this signature.
Signature Type	NETWORK
Signature Structure	COMPOSITE
Implementation	CONTEXT

Affected

Affected Operating Systems

Operating System	Versions
Generic Unix	Any
All Windows [PATCH]	Any
Bay OS [PATCH]	Any
Cisco IOS [PATCH]	Any

Affected Services

Name	Type	Ports	RPC
IP	Networking		

External

Advisories

Advisory Name	Advisory Source
CERT. Advisory CA-98.01 (smurf) IP Denial-of-Service Attacks>>Read	CERT
I-021A: (smurf) IP Denial-of-Service Attacks>>Read	CIAC

Aliases

Vendor	Product	Alias
Publicly Known Names	Public	Smurf

ANEXO 260

CISCO IDS SENSOR SOFTWARE VERSION 4.0

Introduction

Cisco IDS Sensor Software Version 4.0 (Cisco IDS 4.0) is the core of the Cisco Intrusion Detection System, providing unprecedented security. It is designed to accurately identify and classify known and unknown threats targeting your network, including worms, Denial of Service, and application attacks. The first step in delivering an efficient and secure intrusion protection system is accurately detecting all possible threats. To achieve this goal, multiple detection methods are employed, thus ensuring comprehensive coverage. The methods include: stateful pattern recognition, protocol analysis, traffic anomaly detection, and protocol anomaly detection. In addition, Cisco IDS 4.0 provides the capability to prevent detected attacks from executing. And, several ease of use features are integrated to maximize efficiency.

Toolkit: F

Related T
Software /
Dynamic (

Comprehensive Threat Protection

- **Multiple Detection Methods**--Cisco IDS uses an array of detection methods to accurately detect nearly all potential threats. Building on seven years of IDS experience, Cisco delivers a hybrid system using detection methods most appropriate for the threat including stateful pattern recognition, protocol analysis, traffic anomaly detection, and protocol anomaly detection. Cisco IDS 4.0 delivers enhancements to these detection methods, most notably in the area of protocol anomaly detection. Additionally, Cisco IDS delivers a Layer 2 signature engine to provide protection from ARP spoofing techniques in layer 2 environments. These advanced detection techniques, coupled with IP defragmentation, TCP streams reassembly, anti-IDS evasion protection, and deobfuscation techniques, provide comprehensive protection against an array to threats allowing users to quickly identify and mitigate potential damage to data or networked assets.
- **Extensive Protocol Monitoring**--Cisco IDS 4.0 can monitor all of the major TCP/IP protocols, including, but not limited to 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.
- **Comprehensive Attack Detection**--The Cisco IDS 4.0 has the most extensive and comprehensive capability to detect attacks in all of the following categories:
    - ExploitsActivity indicative of someone attempting to gain access or compromise systems on your network, such as Back Orifice, failed login attempts, and TCP hijacking
    - DoSActivity indicative of someone attempting to consume bandwidth or computing resources to disrupt normal operations, such as Trinoo, TFN, and SYN floods
    - ReconnaissanceActivity indicative of someone probing or mapping your network to identify "targets of opportunity," such as ping sweeps and port sweeps; usually a precursor to an actual exploit attempt
    - MisuseActivity 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 IDS to send an alarm on and eliminate any connection that transmits the phrase "XYZ Confidential" in e-mail or File Transfer Protocol (FTP).

Damage Prevention

Cisco IDS uses multi-layer protection options to prevent an attack from successfully reaching the target. After the attack is accurately identified and classified, the system can stop the attack before damage occurs. Whether dropping the packet, terminating the session, reconfiguring ACLs on routers and switches, or dynamically modifying the firewall policy to "shun" the intruder, Cisco IDS offers an array of immediate response actions to stop attacks that can cost you time and money. Cisco IDS 4.0 enhances these techniques by providing added levels of granularity to the way in which these response actions can be configured by extending its capability to include shunning by source/destination port number in addition to source/destination IP address.

Ease of Use

- **Flexible Policy Language**–Because the security objectives for each IDS deployment are unique, Cisco IDS allows users to create and modify policies to specifically suit the environment in which they are deployed. Using our innovative T.A.M.E. (Threat Analysis Micro Engine) policy language, users have the flexibility to create new policies or modify existing policies to meet their unique security objectives. Since T.A.M.E. policies are decoupled from the sensing application, changes do not effect the sensor performance or reliability. Unlike other security languages that rely on simple pattern matching, Cisco T.A.M.E language allows user to leverage the underlying protocol analysis capabilities. Cisco IDS 4.0 simplifies the policy management with improved navigation allowing global changes to be implemented across categories. Additionally, Cisco IDS 4.0 now provides detailed information about the alarm trigger providing the user with forensics data and advanced analysis data to speed the decision support process.
- **Automated Updates Streamlines Management**–Cisco IDS Active Update technology automates the process of updating deployed sensors thus reducing the operating costs. This process provides a facility to automatically distribute new signature files and application upgrades to sensors without operator involvement. Utilizing a secure staging technique, new signature files are placed on a central server and passed to the sensor at scheduled intervals. After verifying the integrity of the package, the sensor automatically installs the update. This new capability significantly streamlines the process of regularly updating remote sensors, thereby lowering the recurring operational costs associated with this task. Additionally, users can subscribe to Cisco Active Update notification services to stay informed about breaking vulnerability news and posted countermeasures. These policy updates are developed and maintained by Cisco's Countermeasures Research Team (C-CRT). This elite team of "white hat" security professionals is dedicated to rapid response to new and evolving threats.

Technical Documentation

Quick Start

(All Cisco IDS Sensor Software Quick Start)

Quick Start Guide for the Cisco Intrusion Detection System Version 4.0

Release Notes

(All Cisco IDS Sensor Software Release Notes)

Release Notes for the Cisco Intrusion Detection System Version 4.0

TECHNICAL SUPPORT

Cisco Secure Encyclopedia

HTTP cgi-phf

General

Key Attributes

Attributes/Severity	**High Severity**
Vulnerability Type:	Network
Exploit Type:	Access

Description
Hypertext Transfer Protocol (HTTP) is the application protocol used by the World Wide Web. HTTP defines how messages are formatted and transmitted and what actions Web servers and browsers should take in response to various commands.

Some versions of Web servers include a CGI library function, escape_shell_cmd(), which can allow attackers to execute commands and access files on the server. The most common example is a sample CGI program called "phf" that often comes precompiled as a default on many NCSA and Apache distributions. This program is vulnerable to the attacks mentioned above, and the vulnerability has been widely exploited. Note that sites that have upgraded the server software, but have not removed or patched vulnerable CGI programs, will still be at risk.

Consequences
Attackers can run arbitrary commands on a Web server as the effective user id (euid) of the httpd server process and access any world-readable files. This can lead to further system access (including root access) and malicious activity.

Countermeasures
NCSA no longer supports NCSA httpd. Cisco recommends upgrading to the latest version of a supported server such as Apache, which is available at the following URL: http://www.apache.org.

For more information about NCSA, refer to the following URL: http://www.ncsa.uiuc.edu/.

Products
IDS Signature WWW Phf Attack

SignatureId/ SubId	3200/0
CSID Versions:	2.1.1
Signature Description	Triggers when the phf attack is detected. This may indicate an attempt to illegally access system resources.
Alarm Level	4
Benign Triggers	This cgi program introduces significant security problems and should be removed. No valid reason to access this file exists.
Signature Type	NETWORK
Signature Structure	COMPOSITE
Implementation	CONTENT

Scanner xxx
CSS Versions: 2.0

Statistics

Statistical Data - for Hosts with HTTP service enabled

Industry Vertical	Percentage of Hosts with this Vulnerability		Percentage of Hosts with Service Vulnerable	
Perspective	**Internal**	**External**	**Internal**	**External**
Advanced Technology				33.33%
Aerospace				66.67%
Photography				28.57%
Computers	0.05%	0.19%	22.36%	15.98%
Computers	0.08%		29.15%	18.59%
Electronics/Chips			37.84%	54.55%
Software		0.48%	10.07%	10.05%
Consumables			44.89%	50.00%
Food/Beverage			44.89%	50.00%
Financial Services			37.22%	1.86%
Banking			54.93%	8.96%
Finance			29.18%	1.01%
Insurance			60.27%	61.54%
Healthcare			58.24%	59.89%
Healthcare			46.67%	62.50%
Pharmaceuticals			59.11%	36.84%
Industrial			52.33%	47.94%
Building Materials			55.00%	
Construction			36.84%	94.44%
Forest/Paper				56.82%
Industrial Equipment				39.84%
Internet			26.83%	44.00%
Internet/Web			26.83%	44.00%
Other			33.59%	36.99%
International			33.59%	51.85%
Unspecified				28.26%
Public Sector			34.38%	61.90%
Education			58.87%	86.36%
Government			31.10%	35.00%
Retail			36.51%	63.33%
Furniture			36.51%	63.33%
Service/Information			17.37%	28.21%
Advertising			23.91%	
Media/Entertainment				28.57%
Outsource Services			10.00%	9.09%

Services			16.67%	100.00%
Transportation			8.33%	50.00%
Motor Vehicles/Parts			100.00%	100.00%
Transportation			5.71%	
Utilities	0.09%		30.11%	22.43%
Energy			29.57%	22.22%
ISP			1.67%	27.74%
Telco	0.12%		31.64%	4.44%
Utilities			90.00%	
Overall	**0.02%**	**0.03%**	**39.96%**	**17.80%**

Affected

Affected Operating Systems

Operating System	Versions
Generic Unix	Any

Affected Software and Programs

Software	Versions	Program	Versions
		cgi-phf	Any
		NCSA [PATCH]	1.3,1.5a
		Apache [PATCH]	1.03

Affected Services

Name	Type	Ports	RPC
HTTP	Web	80/TCP 8080/TCP	

External Links

General Information
General Information
General Information

Aliases

Vendor	Product	Alias
Network Associates Inc.	Cybercop	WWW PHF CHECK

HTTP cgi-finger

General

Key Attributes

Attributes/Severity	**Low Severity**
Vulnerability Type:	Network
Exploit Type:	Recon

Description
The cgi-finger script acts like the finger command. The user names and account information revealed by finger can be used by an intruder to plan future attacks. Finger queries may be directed to other systems from a cgi-finger server, thereby allowing attackers to perform reconnaissance using a Web server to launch the attack.

The finger.pl version of the script can possibly be used to execute commands on the web server.

Consequences
The problem of gaining access to a system is diminished once the attacker has obtained valid user names with which to work. Armed with this information, an attacker may be able to identify which accounts are active and inactive, in order to choose target accounts that are best suited to his or her purpose.

Countermeasures
Remove all unnecessary CGI scripts from the cgi-bin or scripts directory.

Access

Access Required:	network
Access Gained:	None

Discovery Date
01-FEB-1997

Products

IDS Signature WWW finger attempt

SignatureId/ SubId	3232/0
CSID Versions:	2.1.1.6
Signature Description	This signature triggers when an attempt is made to run the finger.pl program via the http server.
Alarm Level	3
Benign Triggers	This signature can be triggered by legitimate as well as illegitimate use of the finger script. It is recommended that all unnecessary CGI scripts be removed from the cgi-bin directory.
Signature Type	NETWORK
Signature	

Structure COMPOSITE
Implementation CONTENT
IDS Signature WWW finger attempt
SignatureId/ SubId 5039/0
CSID Versions: 2.2.1.1
Signature Description This signature triggers when an attempt is made to run the finger program via the http server. It is recommended that all unnecessary programs be removed from the cgi-bin directory.
Alarm Level 3
Benign Triggers No known triggers.
Signature Type NETWORK
Signature Structure COMPOSITE
Implementation CONTENT
Scanner xxx
CSS Versions: 2.0

Statistics

Statistical Data - for Hosts with HTTP service enabled

Industry Vertical	Percentage of Hosts with this Vulnerability		Percentage of Hosts with Service Vulnerable	
Perspective	**Internal**	**External**	**Internal**	**External**
Advanced Technology				33.33%
Aerospace				66.67%
Photography				28.57%
Computers	0.05%	0.38%	22.36%	15.98%
Computers	0.08%		29.15%	18.59%
Electronics/Chips			37.84%	54.55%
Software		0.96%	10.07%	10.05%
Consumables			44.89%	50.00%
Food/Beverage			44.89%	50.00%
Financial Services	0.07%		37.22%	1.86%
Banking			54.93%	8.96%
Finance	0.10%		29.18%	1.01%
Insurance			60.27%	61.54%
Healthcare			58.24%	59.89%
Healthcare			46.67%	62.50%
Pharmaceuticals			59.11%	36.84%
Industrial			52.33%	47.94%
Building Materials			55.00%	
Construction			36.84%	94.44%
Forest/Paper				56.82%
Industrial Equipment				39.84%
Internet			26.83%	44.00%
nternet/ Web			26.83%	44.00%
Other			33.59%	36.99%
International			33.59%	51.85%

Unspecified				28.26%
Public Sector	0.10%		34.38%	61.90%
Education			58.87%	86.36%
Government	0.11%		31.10%	35.00%
Retail			36.51%	63.33%
Furniture			36.51%	63.33%
Service/Information			17.37%	28.21%
Advertising			23.91%	
Media/Entertainment				28.57%
Outsource Services			10.00%	9.09%
Services			16.67%	100.00%
Transportation			8.33%	50.00%
Motor Vehicles/Parts			100.00%	100.00%
Transportation			5.71%	
Utilities			30.11%	22.43%
Energy			29.57%	22.22%
ISP			1.67%	27.74%
Telco			31.64%	4.44%
Utilities			90.00%	
Overall	**0.02%**	**0.06%**	**39.96%**	**17.80%**

Affected

Affected Operating Systems

Operating System	Versions
Generic Unix	Any

Affected Software and Programs

Software	Versions	Program	Versions
		cgi-finger	Any

Affected Services

Name	Type	Ports	RPC
HTTP	Web	80/TCP 8080/TCP	

External

CVE Information

CVE ID: CVE-2000-0128

Advisories

Advisory Name	Advisory Source
Stock fingerd running>>Read	ISS
Finger service>>Read	ISS
Finger Server Pipe Vulnerability>>Read	BUGTRAQ

Links

General Information
General Information
Advisory
Fix
Exploit, Solution & Discussion
Exploit

Aliases

Vendor	Product	Alias
Network Associates Inc.	Cybercop	WWW FINGER CHECK

SiteWare Editor Desktop Directory Traversal Vulnerability

General Affected External

General

Key Attributes

Attributes/Severity	**Medium Severity**
Vulnerability Type:	NONE
Exploit Type:	NONE

Description
SiteWare Editor Desktop is the web-based administration tool for managing Screaming Media content. Screaming Media is a provider for custom web content.

There exists a vulnerability that will allow an attacker to execute a directory traversal against SiteWare Editor Desktop. The attacker could obtain read access to web server-readable files which could help in future attacks.

Consequences
Attacker could read all web server-readable files.

Countermeasures
Update SiteWare to the latest patch available from Screaming Media.

Access

Access Required:	web access
Access Gained:	Read access to web server-readable files

Discovery Date
13-JUN-2001

Products

IDS Signature WWW SiteWare Editor Directory Traversal

SignatureId/ SubId	5155/0
CSID Versions:	Any
Signature Description	Alarms if SWEditServlet is called with a ../ as an argument
Alarm Level	3
Benign Triggers	No known triggers.
Signature Type	NETWORK
Signature Structure	ATOMIC
Implementation	CONTENT

Affected Software and Programs

Software	Versions	Program	Versions
		SiteWare [PATCH]	2.5,2.501,3.0,3.01,3.02,3.1

To update a sensor from sensor software 3.x to sensor software 4.x, you must have physical access to that sensor so that you can re-image it.

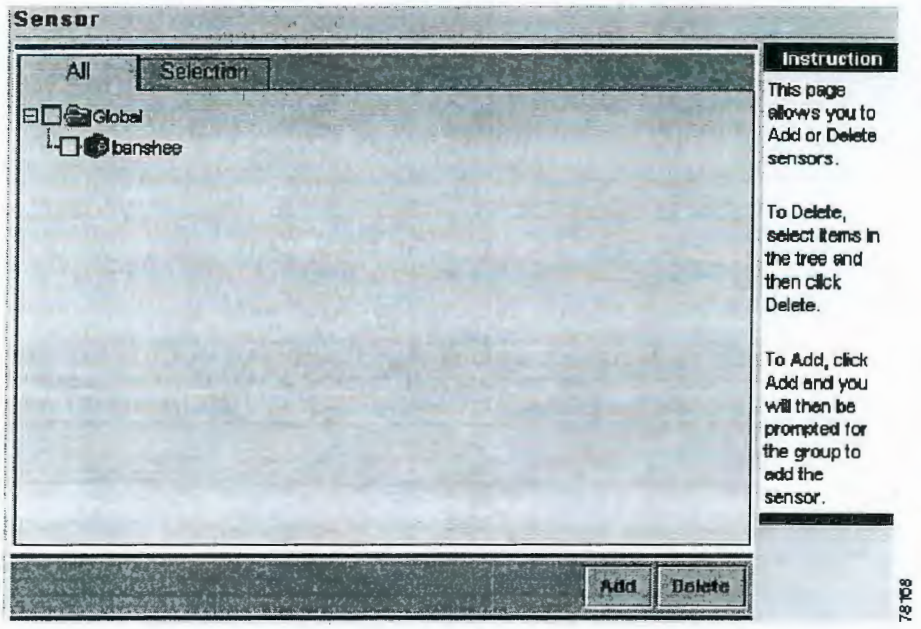
Note After updating sensor software versions and signature release levels, you cannot revert to the previous version or level using the IDS MC.

To update your sensor software version and signature release level, follow these steps:

Step 1 Determine the sensor software version and signature release level that your server is operating with. For a Security Monitor server, do not perform this step because it is not necessary. For an IDS MC server, proceed with Step a.

a. In IDS MC, select **Devices > Sensor**.

The Sensor page appears.

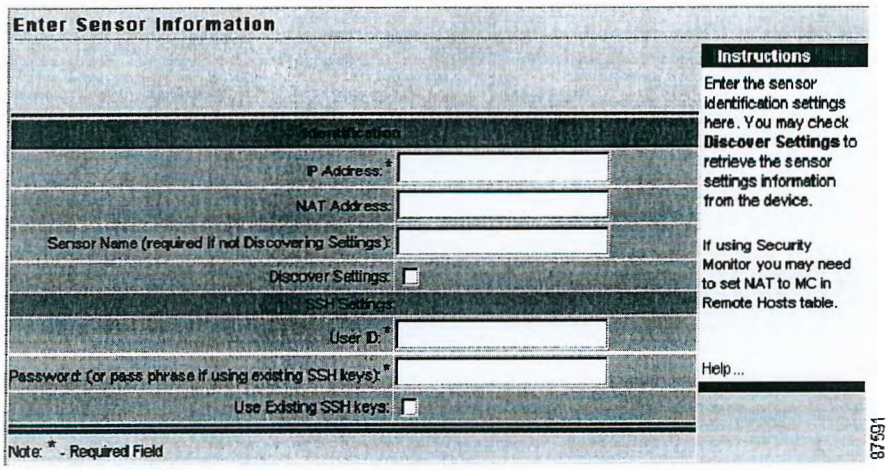


b. Click **Add**.

The Select Group page appears.

c. Select any group, and then click **Next**.

The Enter Sensor Information page appears.



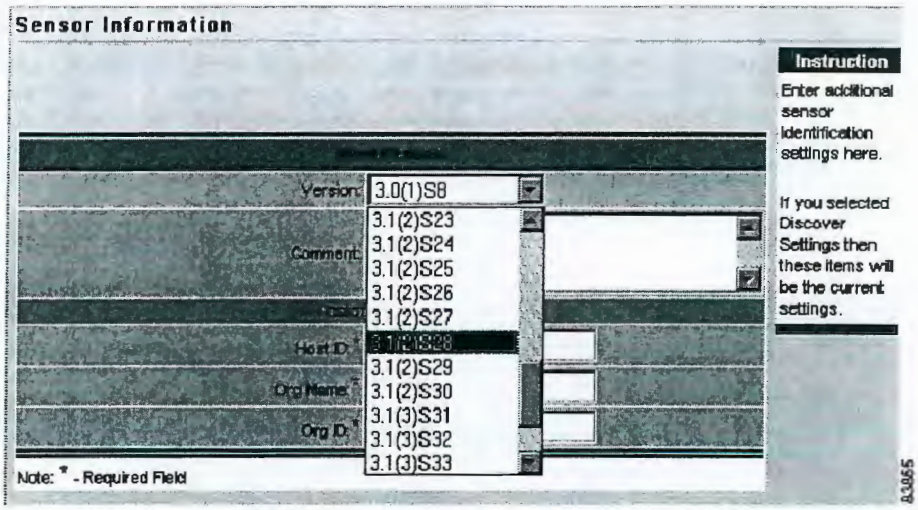
d. Enter an IP address, a sensor name, a user ID, and a password as if you were adding a sensor; however, you will not complete the addition of a sensor in this step of this procedure. You will only determine the sensor software and signature version that your IDS MC server is operating with.

e. Click **Next**.

The Sensor Information page appears.

f. Display the Version list.

A scrolling list appears. This list displays all the sensor software and signature versions that your IDS MC server is operating with.



g. Click **Cancel**. (The purpose of performing this step is to determine the sensor software and signature versions that your IDS MC server is operating with, not to complete the process of adding a sensor.)

Step 2 Determine the sensor software version(s) and signature release level(s) that your sensors are using. For a Security Monitor server, do not perform this step because sensors are not (and cannot be) updated through Security Monitor. For an IDS MC server, proceed with Step a.

a. In the IDS MC, select **Configuration > Settings**.

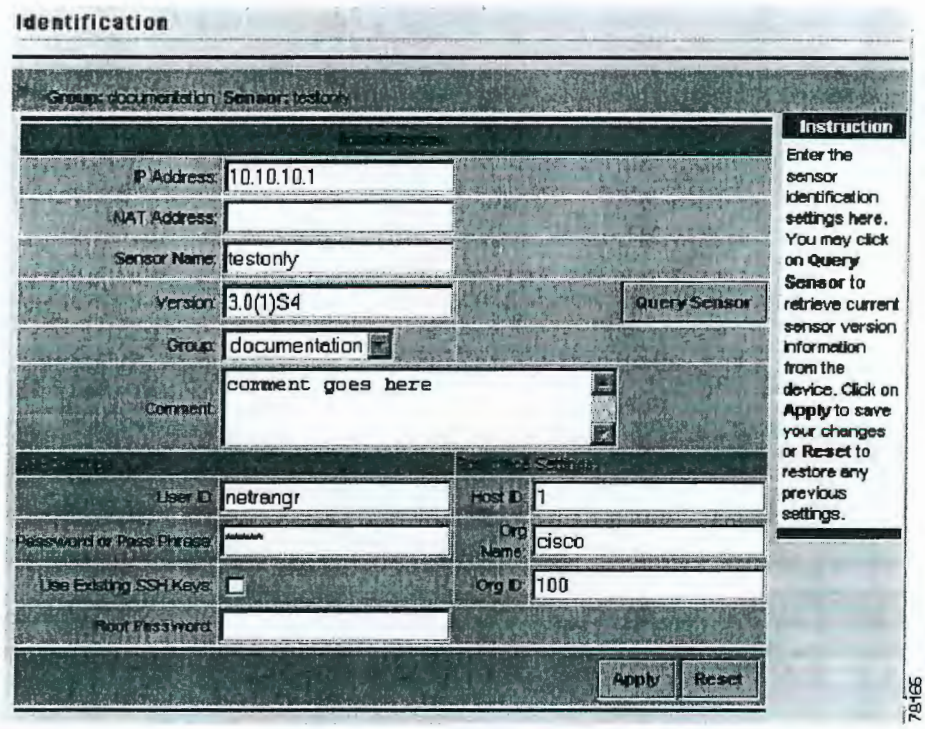
b. Click the **Object Selector** handle.

c. From the Object Selector, select the sensor whose sensor software and signature version you want to determine.

   The Object Selector closes.

d. From the TOC, select **Identification**.

   The Identification page appears, and the Object bar displays the sensor you selected from the Object Selector. The sensor software and version of the sensor appear in the Version field. In this example, the version is `3.0(1)S4`.



Step 3 Check the Cisco Systems Software Center to see if an update file is available. Update files are explained in detail in the introduction to this procedure. Each update file has a readme file associated with it to provide additional details.

a. If you are registered with Cisco.com, and you have logged in, and you are authorized for Cisco Secure IDS Strong Crypto software, navigate to http://www.cisco.com/cgi-bin/tablebuild.pl/mgmt-ctr-ids; then skip to Step e in this step. Otherwise, proceed with Step b.

b. Register with Cisco.com at http://www.cisco.com and log in.

c. Submit an application to download Cisco Secure IDS Strong Crypto Software if you are not already authorized. The approval process typically takes a few hours.

d. Navigate to http://www.cisco.com/kobayashi/sw-center/sw-cw2000.shtml and follow the link to `Management Center for IDS Sensors` under `VPN/Security Management Solution`.

(The navigation path is www.cisco.com > [log in] > Technical Support > Software Center > Cisco Works Software > Management Center for IDS Sensors.)

Tip Use this download location for the IDS MC and Security Monitor both.

e. Click on the name of an update file to download.

The Software Download page appears.

Step 4 Download the update file to `~CSCOpx/mdc/etc/ids/updates` on the server.

Note Do not change the name of the update file. Also, do not extract (unzip) the update file.

Step 5 Choose one of the following:

- To update your IDS MC server only, proceed with Step 6 of this procedure.
- To update your Security Monitor server only, skip to Step 17.

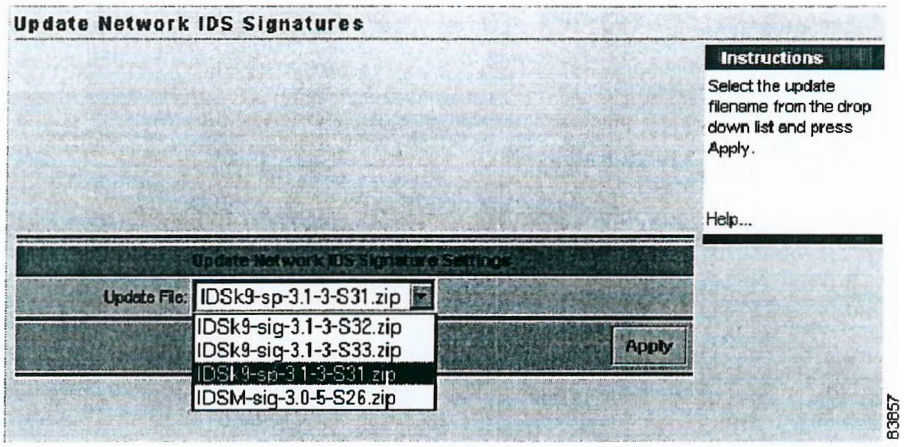
Tip If you have installed the IDS MC and Security Monitor on the same host, your Security Monitor server will be updated when you update your IDS MC server.

- To update a sensor from sensor software 3.x to sensor software 4.x, skip to Step 22.
- To update a sensor *other than from* 3.x to 4.x, proceed with Step 6.
- To update your IDS MC server and a sensor other than from 3.x to 4.x, proceed with Step 6.

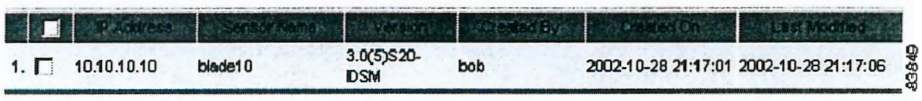
Step 6 In the IDS MC, select **Configuration > Updates**.

Step 7 From the TOC, select **Update Network IDS Signatures**.

The Update Network IDS Signatures page appears, showing all the update files, if any, that have been downloaded to `~CSCOpx/mdc/etc/ids/updates` on the server where you have installed the IDS MC.

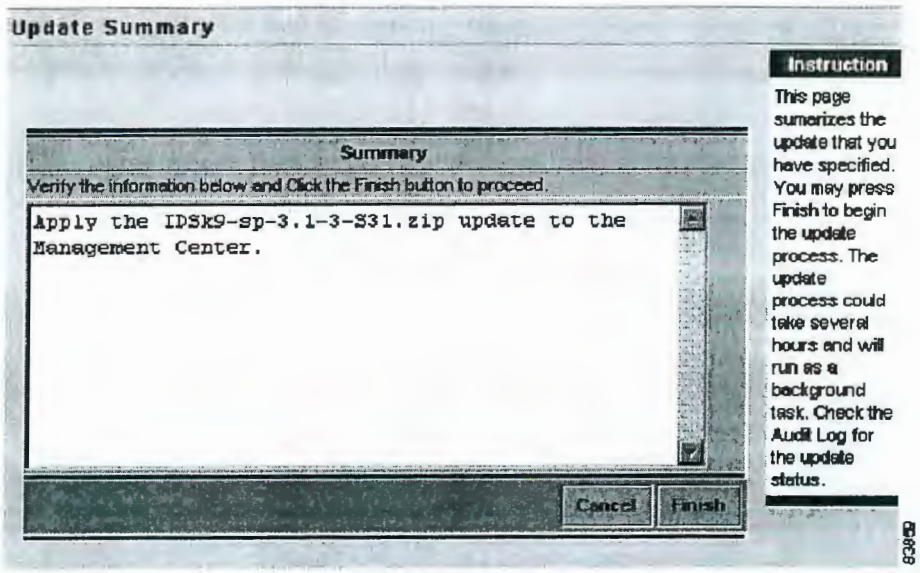


Step 8 Assume for this example that your IDS MC installation contains one IDS module, as illustrated here.



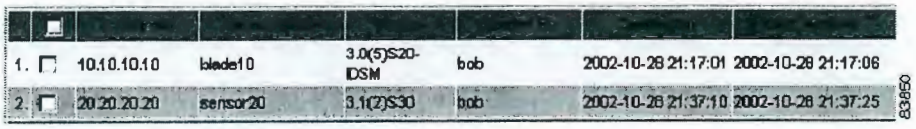
Select an update file, `IDSk9-sp-3.1-3-S31.zip` in this example, from the Update File list, and then click **Apply**.

The Update Summary page appears. It states that the update file will be applied to IDS MC. That is because the update file does not apply to any devices in your IDS MC installation. (The update file begins with `IDSk9`, so it applies to sensor appliances, not to IDS modules, and there are no sensor appliances in your IDS MC installation.)



If that is what you want to do, skip to Step 14.

Step 9 To continue this example, assume that you have added a sensor appliance to your IDS MC installation, as illustrated here.



Select the same update file, `IDSk9-sp-3.1-3-S31.zip`, and then click **Apply**.

The Select Sensors to Update page appears. The Select Sensors to Update page displays all the sensors (in any group) that can be updated using the update file you selected, presuming that your server has established communications with them; however, you must select only devices that follow a prescribed update path. In this example, the update file applies to only one device and IDS MC 1.0 is being used, so the Select Sensors to Update page appears as a non-scrolling table. This non-scrolling table does not appear if IDS MC 1.1 is being used or if you are updating more than one sensor.

Affected Services

Name	Type	Ports	RPC
HTTP	Web	80/TCP 8080/TCP	

External Advisories

Advisory Name	Advisory Source
FS-061201-19-SMSW>>Read	Foundstone
CAN-2001-0555>>Read	CVE Candidate

Links

Manufacturer
Exploit, Solution & Discussion
General Information

BUSINESS STRATEGIES & SOLUTIONS | NETWORKING SOLUTIONS & PROVISIONED SERVICES | P
TECHNOLOGIES | ORDERING | TECHNICAL SUPPORT | LEARNING & EVENTS | PARTNERS & RESEL
Home | Logged In | Profile | Contacts & Feedback | Site Help

TECHNICAL SUPPORT

Cisco Secure Encyclopedia

Code Red Internet Worm (CRv1, CRv2, and CRII)

General Affected External

General

Key Attributes

Attributes/Severity	**High Severity**
Vulnerability Type:	Network
Exploit Type:	Access

Description

There are several variants of a computer worm, known as "Code Red", which are spreading across the Internet and on the internal networks of many organizations. This has resulted in widespread computer infestations, and denial of service to computer networks due to the excessive amounts of network traffic generated by infected systems port scanning for new systems to infect.

The initial "Code Red" worm exploited a buffer overflow vulnerability in the Indexing Service of Microsoft's IIS web server (version 4.0 and 5.0). It then executed malicious code to install itself into the infected host's memory and scan for other hosts to infect.

Code Red, version 1 used a random number generator with a static seed to generate a limited number of IP addresses to scan. Code Red, version 2 uses a random number generator with a random seed to generate larger numbers of IP addresses to scan (approx. 2,000 hosts per minute). If the infected web server were improperly configured the worm would also deface the web site. On the 20th day of the month all infected hosts would attempt a denial of service attack against "www.whitehouse.gov" by flooding its IP address.

Code Red II, affects only Windows 2000 hosts, it does not deface web sites nor attempt denial of service attacks. When it infects a host, it first determines if the system has already been infected by CRv1 or CRv2. If not, the worm executes its own malicious code that creates an administrator equivalent "backdoor" into the infected host system. It also installs a trojan copy of explorer.exe that allows an attacker to access the C: and D: root directories from the Internet via a virtual web directory.

Unlike CRv1 and CRv2, CodeRed II is not memory resident, therefore rebooting an infected host does not remove CodeRed II.

Consequences

Networks infected with the "Code Red" worm may experience significant performance issues due to the high amounts of network traffic generated by the infected hosts scanning for new hosts to infect.

Instances of CRv1 and CRv2 will attempt to deface improperly configured web servers and/or attempt to flood "www.whitehouse.gov".

Instances of CRII will install a "backdoor" with administrative privileges and/or create virtual web directories to the root directory of C: and D: that would allow an attacker to execute commands and/or retrieve sensitive

information (ie. passwords, credit card numbers, etc)

Countermeasures
It is highly recommended that organizations ensure that all of their Windows NT / 2000 hosts running IIS (version 4.0 and 5.0) are patched to prevent the Code Red worm from infecting their network.

Apply the Microsoft patch referenced in Security Bulletin MS01-044 (IIS Cumulative Patch) to mitigate the affects of CRv1, CRv2, and CRII. In addition, apply the patch referenced in Security Bulletin MS00-052 (Relative Shell Path) to mitigate the affects of the trojanized "Explorer.exe" file.

Ensure all network shares and user accounts are legitimate and disable any "backdoors" or virtual web directories created by Code Red II.

Access

Access Required:	Network connectivity to the vulnerable web server.
Access Gained:	System level access to the web server.

Discovery Date
17-JUL-2001

Products
IDS Signature WWW IIS .ida Indexing Service Overflow

SignatureId/ SubId	5126/0
CSID Versions:	Any
Signature Description	This vulnerability will alarm if web traffic is detected with the ISAPI extension of .ida? and a data size of greater 200 chars.
Alarm Level	5
Benign Triggers	No known triggers.
Signature Type	NETWORK
Signature Structure	ATOMIC
Implementation	CONTENT
Scanner CSS Versions:	2.0.2.3

Related Vulnerabilities

ID	Descriptive Name
3394	Microsoft IIS IDA/ISAPI Indexing Service Buffer Overflow

Affected
Affected Operating Systems

Operating System	Versions
Windows NT [PATCH]	4.x
Windows 2000 [PATCH]	Any
Windows NT Server [PATCH]	4.x
Windows 2000 Server [PATCH]	Any

Affected Software and Programs

Software	Versions	Program	Versions
Internet Information Server (IIS) [PATCH]	4.0/5.0		

Affected Services

Name	Type	Ports	RPC
HTTP	Web	80/TCP 8080/TCP	

External

Advisories

Advisory Name	Advisory Source
All versions of Microsoft Internet Information Services Remote buffer overflow (SYSTEM Level Access) >>Read	Eeye
.ida "Code Red" Worm>>Read	Eeye
CA-2001-19 "Code Red" Worm Exploiting Buffer Overflow In IIS Indexing Service DLL>>Read	CERT
"Code Red" Worm - Customer Impact>>Read	Cisco PSIRT
CA-2001-23 Continued Threat of the "Code Red" Worm>>Read	CERT
.ida "Code Red" Worm>>Read	Eeye
MS Index Server and Indexing Service ISAPI Extension Buffer Overflow Vulnerability>>Read	BUGTRAQ
CA-2001-13 Buffer Overflow In IIS Indexing Service DLL>>Read	CERT
CodeRedII Worm Analysis>>Read	Eeye
CAN-2001-0500>>Read	CVE Candidate
IIS idq.dll ISAPI extension buffer overflow>>Read	ISS

Links

General Information
General Information
Fix
Fix
Fix
Fix
Fix

Aliases

Vendor	Product	Alias
ISS XForce	XForce Database	iis-isapi-idq-bo
ISS XForce	XForce Database	backdoor-codered2

DNS Spoofing

General Affected External

General

Key Attributes

Attributes/Severity	**High Severity**
Vulnerability Type:	Network
Exploit Type:	Access

Description
Domain Name Service (DNS) spoofing is simply tricking the DNS system into believing your domain name is something other than it really is. Successful DNS spoofing allows malicious attackers to circumvent authentication based on hostname, gain access to another site's e-mail, redirect users to different websites, and initiate denial-of-service attacks.

Consequences
A malicious user can gain access to systems using hostname resolution for authentication, redirect users or e-mail to different sites, or conduct denial-of-service attacks.

Countermeasures
Use the latest vesion of BIND. Apply all the latest recommended patches from your DNS server vendor.

Access

Access Required:	Network
Access Gained:	Depending on the type of DNS spoofing attack, a malicious user could gain host access, redirect users to different sites, or read e-mail.

Discovery Date
15-FEB-1996

Affected

Affected Operating Systems

Operating System	Versions
Generic Unix	Any
Generic Linux	Any
Windows NT Server [PATCH]	Any
Windows 2000 Server [PATCH]	Any

Affected Software and Programs

Software	Versions	Program	Versions
DNS [PATCH]	Any		

Affected Services

Name Type	Ports	RPC

DNS	Info_status	53/TCP 53/UDP
BIND	Application	53/TCP 53/UDP

External
CVE Information
CVE ID: CVE-1999-0024

Advisories

Advisory Name	Advisory Source
DNS spoofing/registering/etc>>Read	BUGTRAQ
CERT(sm) Advisory CA-96.02>>Read	CERT
CERT. Advisory CA-1997-22 BIND>>Read	CERT

Links
Exploit, Solution & Discussion
General Information

Aliases

Vendor	Product	Alias
ISS XForce	XForce Database	nt-poison-dns

TECHNICAL SUPPORT

Cisco Secure Encyclopedia

Quick Search: GO Advanced Search

SeaGlass Technologies sqlMerchant Directory Traversal

General Affected External

General

Key Attributes

Attributes/Severity	**Medium Severity**
Vulnerability Type:	Network
Exploit Type:	Recon

Description
sqlMerchant is a suite of cgi scripts to enable web commerce, written by SeaGlass Technologies.

A problem exists with one of the included scripts that will allow a malicious user to conduct a directory traversal recon attack.

Recon attacks are useful in gaining knowledge for future attacks.

Consequences
An attacker may gain information that could lead to future attacks.

Countermeasures
None at this time.

Access

Access Required:	web access
Access Gained:	View directory structure of underlying webserver

Discovery Date
08-SEP-2001

Products
IDS Signature sgiMerchant Directory Traversal

SignatureId/ SubId	5180/0
CSID Versions:	Any
Signature Description	This sig will fire when the file view_item is accessed with a parameter of html_file that has a value containing a '../'.
Alarm Level	3
Benign Triggers	No known triggers.
Signature Type	NETWORK
Signature Structure	ATOMIC
Implementation	CONTENT

Affected Services

Name	Type	Ports	RPC
http	Web	80/TCP	

External Links
Exploit, Solution & Discussion

Aliases

Vendor	Product	Alias
Security Focus	Vulnerabilities Database	SeaGlass Technologies sglMerchant Directory Traversal Vulnerability
ISS XForce	XForce Database	sglmerchant-dot-directory-traversal

Search:
GO
Search All Cisco.com
Toolkit: Roll over tools below
Feedback | Help

Related Tools
TAC Case Open
TAC Case Query
TAC Case Update
Dynamic Configuration Tool

BUSINESS STRATEGIES & SOLUTIONS | NETWORKING SOLUTIONS & PROVISIONED SERVICES | P
TECHNOLOGIES | ORDERING | TECHNICAL SUPPORT | LEARNING & EVENTS | PARTNERS & RESEI
Home | Logged In | Profile | Contacts & Feedback | Site Help

Cisco Secure Encyclopedia

chargen DoS

General Affected External

General

Key Attributes

Attributes/Severity	**Medium Severity**
Vulnerability Type:	Network
Exploit Type:	Denial

Description
UNIX and Windows NT systems that have the chargen service enabled are susceptible to denial-of-service attacks. The chargen service runs on TCP and UDP ports 19 and is one of the simple TCP/IP services. Its only function is generating a constant stream of ASCII characters.

The attack consists of sending a flood of UDP packets from a spoofed source IP address to the subnet broadcast address with the destination port set to 19. The system running chargen responds to each broadcast, creating a flood of UDP packets in an infinite loop. By connecting the chargen port on a host to the echo port on another host, an attacker can cause a denial of service.

Consequences
A remote attacker can initiate an attack that can consume increasing amounts of network bandwidth, resulting in a loss of performance or a denial of service.

Countermeasures
Disable the chargen and echo services on all machines.

Products
Scanner xxx
CSS Versions: 2.0
IDS Signature Chargen Echo DoS

SignatureId/ SubId	4061/0
CSID Versions:	Any
Signature Description	This signature detects packets destined for the UDP echo (7) port with the chargen (19) service as the source port. This will result in the contents of the packet being "echoed" back to the source IP address, which may be spoofed.
Alarm Level	3
Benign Triggers	There are no known benign triggers.
Signature Type	NETWORK
Signature Structure	ATOMIC
Implementation	CONTENT

IDS Signature Chargen DoS

SignatureId/ SubId	4052/0
CSID Versions:	2.1.1.6

Signature Description	This signature triggers when a UDP packet is detected with a source port of 7 and a destination port of 19.
Alarm Level	3
Benign Triggers	No known triggers.
Signature Type	NETWORK
Signature Structure	ATOMIC
Implementation	CONTEXT

Affected

Affected Operating Systems

Operating System	Versions
Windows NT [PATCH]	4.0
Generic Unix	Any

Affected Software and Programs

Software	Versions	Program	Versions
		chargen	Any

Affected Services

Name	Type	Ports	RPC
Chargen	Info_status	19/TCP 19/UDP	

External

CVE Information

CVE ID: CVE-1999-0103

Advisories

Advisory Name	Advisory Source
UDP Port Denial-of-Service Attack>>Read	CERT

Links

General Information

Fix

Aliases

Vendor	Product	Alias
Publicly Known Names	Public	chargen
Publicly Known Names	Public	chargen flood

Multiple ISC BIND Denial of Service Vulnerabilities

General Affected External

General

Key Attributes

Attributes/Severity	**Medium Severity**
Vulnerability Type:	Network
Exploit Type:	Denial

Description
BIND is the software used to provide domain name resolution services. It has several denial-of-service vulnerabilities that could allow remote malicious users to cause site DNS services to be stopped.

One documented bug (zxfr) in the ISC BIND code allows users with zone transfer privileges to crash vulnerable name servers.

Another bug in BIND (srv) contains a Denial of Service vulnerability that can cause affected DNS servers to go into an infinite loop.

Consequences
Arbitrary remote hosts can cause DNS servers to become disabled.

Countermeasures
Update BIND to version 8.2.2-P7 or restrict zone transfers to trusted hosts.

Access

Access Required:	None
Access Gained:	None

Discovery Date
13-NOV-2000

Products
Scanner
CSS Versions: 2.0.2.3
IDS Signature DNS SRV DoS

SignatureId/ SubId	6058/0
CSID Versions:	Any
Signature Description	Alarms when a DNS query type SRV and DNS query class IN is detected with more than ten pointer jumps in the SRV resource record.
Alarm Level	5
Benign Triggers	No known triggers.
Signature Type	NETWORK
Signature Structure	ATOMIC
Implementation	CONTENT

Affected Software and Programs

Software	Versions	Program	Versions
BIND [PATCH]	8.x.x		

Affected Services

Name	Type	Ports	RPC
BIND	Application	53/TCP 53/UDP	

External Advisories

Advisory Name	Advisory Source
CERT Advisory CA-2000-20 Multiple Denial-of-Service Problems in ISC BIND>>Read	CERT

Links

Manufacturer

TECHNICAL SUPPORT
Cisco Secure Encyclopedia

TECHNICAL SUPPORT

Cisco Secure Encyclopedia

Quick Search: GO Advanced Search

Toolkit: F
Feedback

Related T
TAC Case
TAC Case
TAC Case
Dynamic (

LPRng Format String Vulnerability

General Affected External

General

Key Attributes

Attributes/Severity	**Medium Severity**
Vulnerability Type:	Network
Exploit Type:	Access

Description
LPRng, the "next generation" of print-service management software now being packaged in several open-source operating system distributions, has a missing format string argument in at least two calls to the syslog() function. Missing format strings in function calls that allow user-supplied arguments to be passed to a susceptible *snprintf() function call may allow remote users with access to the printer port (port 515/tcp) to pass format-string parameters that can overwrite arbitrary addresses in the printing service's address space. Such overwriting can cause segmentation violations leading to denial of printing services or lead to the execution of arbitrary code injected through other means into the memory segments of the printer service.

Consequences
It is possible for a remote user to execute arbitrary code on vulnerable systems. This could lead to denial of print services or system access with elevated privileges.

Countermeasures
Upgrade to non-vulnerable version of LPRng (3.6.25). Disallow access to printer service ports (typically 515/tcp) using firewall or packet-filtering technologies.

Access
Access Required: none
Access Gained: None

Discovery Date
25-SEP-2000

Affected
Affected Operating Systems

Operating System	Versions
FreeBSD [PATCH]	3.5.1,4.1,4.1.1
Redhat Linux [PATCH]	7.0
Caldera Linux [PATCH]	2.3,2.4
Trustix Secure	

Linux [PATCH] 1.0,1.1

Affected Software and Programs

Software	Versions	Program	Versions
LPRng	Any	lpd	Any

Affected Services

Name	Type	Ports	RPC
LPD	Printing	515/TCP	

External Advisories

Advisory Name	Advisory Source
Multiple Vendor LPRng User-Supplied Format String Vulnerability >>Read	SecurityFocus

Links

General Information
General Information
General Information

FTP PORT Relay

General Affected Statistics External

General

Key Attributes

Attributes/Severity	**Medium Severity**
Vulnerability Type:	Network
Exploit Type:	Relay

Description
File Transfer Protocol (FTP) is one protocol by which files can be transferred to and from remote computer systems. The user transferring a file usually needs authority to login and access files on the remote system.

As part of this protocol, a user can input the PORT command to specify the destination address to which FTP data should be sent. Normally, this is the user's machine, but data can be sent to any address.

Attackers could use an FTP server to launch various exploits using the PORT command. This attack is also known as "FTP bounce."

Anonymous FTP servers are especially susceptible to this activity because they do not require user authentication.

Consequences
An attacker could use an FTP server to launch exploits against another machine. If the server is an anonymous FTP server, then the attacker does not require an account on the server to launch the attack. If any hosts or networks allow special access to the FTP server host, then the attacker, via the FTP server, has the same access. An attacker could use this special access or trust to possibly bypass firewalls or create downstream liability if used against another organization.

Countermeasures
Refrain from using an anonymous FTP server unless absolutely necessary.

Access

Access Required:	User or Anonymous
Access Gained:	

Products

IDS Signature FTP Improper Address Specified

SignatureId/ SubId	3153/0
CSID Versions:	2.1.1
Signature Description	Triggers if a port command is issued with an address that is not the same as the requesting host.
Alarm Level	4
Benign Triggers	No known triggers.
Signature Type	NETWORK

Signature Structure ATOMIC
Implementation CONTENT
Scanner xxx
CSS Versions: 2.0

Statistics

Statistical Data - for Hosts with FTP service enabled

Industry Vertical	Percentage of Hosts with this Vulnerability		Percentage of Hosts with Service Vulnerable	
Perspective	**Internal**	**External**	**Internal**	**External**
Advanced Technology		15.00%		45.00%
Aerospace				57.14%
Photography		23.08%		38.46%
Computers	1.87%	3.78%	27.91%	36.22%
Computers	2.82%	7.29%	33.11%	36.46%
Electronics/Chips			3.59%	33.33%
Software	0.14%		21.66%	36.05%
Consumables	48.49%		73.58%	
Food/Beverage	48.49%		73.58%	
Financial Services	4.88%		25.76%	4.33%
Banking	30.21%		64.26%	31.58%
Finance	2.22%		21.79%	3.73%
Insurance	13.33%		36.67%	
Healthcare	29.57%	2.96%	60.46%	39.26%
Healthcare	5.06%	3.01%	63.92%	38.35%
Pharmaceuticals	31.04%		60.26%	100.00%
Industrial	0.30%	25.93%	31.94%	37.04%
Building Materials	0.38%		34.48%	100.00%
Construction			22.97%	
Farm Equipment				50.00%
Forest/Paper		10.00%		20.00%
Industrial Equipment		32.50%		40.00%
Internet	4.05%		23.12%	
Internet/Web	4.05%		23.12%	
Other	34.46%	14.81%	70.06%	29.63%
International	34.46%		70.06%	
Unspecified		16.67%		33.33%
Public Sector	13.25%		38.53%	25.58%
Education	11.76%		55.29%	54.55%
Government	13.37%		37.08%	15.62%
Retail	8.40%	5.88%	49.51%	17.65%
Furniture	8.40%	5.88%	49.51%	17.65%
Service/Information	4.57%		28.57%	45.03%
Advertising	1.08%		10.75%	

Media/Entertainment				44.57%
Outsource Services	5.56%		36.11%	66.67%
Services	10.87%		58.70%	
Transportation			46.15%	
Motor Vehicles/Parts			100.00%	
Transportation			45.56%	
Utilities	7.57%		20.73%	20.77%
Energy			21.38%	12.50%
ISP			47.22%	30.15%
Telco	10.99%		20.47%	4.19%
Utilities	7.69%		17.95%	
Overall	**11.89%**	**1.46%**	**37.84%**	**21.59%**

Affected

Affected Operating Systems

Operating System	Versions
Windows 95 [PATCH]on x86 [PATCH]	Any
Windows NT [PATCH]	Any
Generic Unix	Any

Affected Software and Programs

Software	Versions	Program	Versions
		ftpd	Any

Affected Services

Name	Type	Ports	RPC
FTP	Data_transfer	20/TCP 21/TCP	

External

CVE Information

CVE ID: CVE-1999-0017

Advisories

Advisory Name	Advisory Source
CERT. Advisory CA-97.27.FTP_bounce>>Read	CERT

Links

General Information
General Information
General Information
General Information
Advisory

Aliases

Vendor	Product	Alias
Network Associates Inc.	Cybercop	FTP BOUNCE ATTACK CHECK
Publicly Known Names	Public	FTP bounce

FTP Improper Port

General Affected External

General

Key Attributes

Attributes/Severity	**Medium Severity**
Vulnerability Type:	Network
Exploit Type:	Relay

Description

File Transfer Protocol (FTP) is one protocol by which files can be transferred to and from remote computer systems. The user transferring a file usually needs authority to login and access files on the remote system.

As part of this protocol, a user can input the PORT command to specify the destination address to which FTP data should be sent. The PORT command is part of the FTP specification and is present in all implementations.

Attackers could use an FTP server to launch various exploits using the PORT command. This attack is also known as "FTP bounce."

Anonymous FTP servers are especially susceptible to this activity because they do not require user authentication.

Consequences

An attacker could use an FTP server to launch exploits against another machine. If the server is an anonymous FTP server, then the attacker does not require an account on the server to launch the attack. If any hosts or networks allow special access to the FTP server host, then the attacker, via the FTP server, has the same access. An attacker could use this special access or trust to possibly bypass firewalls or create downstream liability if used against another organization.

Countermeasures

If you need to run an anonymous ftp server, set it up so that users can upload files but not access them. The decision can then be made as to which files can be put into publicly accessible directories. If you have intrusion detection technology, do not allow PORT commands to specify a machine different from the requesting machine.

Access

Access Required: user or anonymous access

Access Gained:

Products

IDS Signature FTP Improper Address Specified

SignatureId/ SubId 3153/0

CSID Versions: 2.1.1

Signature Triggers if a port command is issued with an address that is

Description	not the same as the requesting host.
Alarm Level	4
Benign Triggers	No known triggers.
Signature Type	NETWORK
Signature Structure	ATOMIC
Implementation	CONTENT

IDS Signature FTP Improper Port Specified

SignatureId/ SubId	3154/0
CSID Versions:	2.1.1
Signature Description	Triggers if a port command is issued with a data port specified that is <1024 or >65535.
Alarm Level	4
Benign Triggers	No known triggers.
Signature Type	NETWORK
Signature Structure	ATOMIC
Implementation	CONTENT

Scanner xxx

CSS Versions: 2.0

.

Affected

Affected Operating Systems

Operating System	Versions
Generic Unix	Any
All Windows [PATCH]	Any

Affected Software and Programs

Software	Versions	Program	Versions
		ftpd	Any

Affected Services

Name	Type	Ports	RPC
FTP	Data_transfer	20/TCP 21/TCP	

.

External

CVE Information

CVE ID: CVE-1999-0017

Advisories

Advisory Name	Advisory Source
CERT. Advisory CA-97.27.FTP_bounce>>Read	CERT

Links

General Information

General Information

TECHNICAL SUPPORT

Cisco Secure Encyclopedia

NIMDA Internet Worm

General Affected External

General

Key Attributes

Attributes/Severity	**High Severity**
Vulnerability Type:	Network
Exploit Type:	Access

Description

The NIMDA worm exploits vulnerabilities in Microsoft Internet Information Server (IIS), Internet Explorer (IE), and Outlook (MAPI) to infect workstations running Windows 95/98/ME, workstations running Windows NT/2000, and servers/domain controllers running Windows NT/2000. It uses multiple propagation vectors, including:

1. Client to client via email (malicious code "readme.exe")

2. Client to client via open network shares (malicious code "readme.exe")

3. Client to web server via active scanning and exploitation of Microsoft IIS buffer overflow vulnerabilities (admin.dll uploaded via TFTP)

4. Client to web server via active scanning for the back doors created by "Code Red II" and "sadmind/IIS" worms (root.exe or admin.dll file uploaded, guest account enabled and added to admin group)

5. Web server to client via browsing of compromised web sites (embedded javascript code "readme.eml")

Consequences

Networks infected with the NIMDA worm may experience significant performance issues due to the high amounts of network traffic generated by the infected hosts scanning for new hosts to infect.

NIMDA exploits the "backdoor" created by Code Red II to gain administrative access to the infected host. This could result in the retrieval of the security account manager (SAM) password file.

It enables the guest account and adds it to administrators group of the infected host, including domain controllers.

It scans and modifies registry keys to ensure default shares are available (eg. ADMIN$, C$, D$). Grants full access permissions to the "everyone" group for default shares. Deletes registry subkeys that establish network share security.

It scans open network shares for executable system files and replace them with an infected file of the same name, including files in the dllcache directory (used for Windows File Protection).

It scans open network shares for .ASP, .HTM, and .HTML files, appending malicious javascript code to propagate itself. It also creates a MIME

encoded "readme.eml" file in each directory where it finds .ASP, .HTM, and .HTML files.

It modifies the "system.ini" to allow the worm to execute itself when the infected system is rebooted.

It creates infected *.eml and *.dll files on all open network shares.

Countermeasures
It is highly recommended that organizations patch all Windows NT/2000 hosts running IIS (version 4.0 and 5.0) to mitigate IIS buffer overflows and Code Red II backdoors.

Upgrade to Microsoft Internet Explorer 5.5 SP2 or Internet Explorer 5.01 SP2 to mitigate launching malicious code via HTML or email. Also, consider disabling javascript support in web and email clients.

Apply the Microsoft patch referenced in Security Bulletin MS01-044 (IIS Cumulative Patch) to mitigate the affects of Code Red and NIMDA.

Ensure all network shares and user accounts are legitimate, appropriate file permissions are applied, and disable any "backdoors" created by Code Red II.

Employ ingress and egress filtering on UDP port 69, TCP port 80, and SMB (NetBIOS) to mitigate the propagation of the NIMDA worm to and from the network.

Ensure the latest anti-virus software is being used along with current virus signatures to mitigate NIMDA propagation.

Access

Access Required:	Network connectivity via web client (IE), web server (IIS), or email client (MAPI)
Access Gained:	System level access to infected web servers, administrative level access to infected workstations

Discovery Date
18-SEP-2001

Products
Scanner
CSS Versions: 2.0.2.4

Related Vulnerabilities

ID	Descriptive Name
2965	IIS Unicode Remote Command Execution
3500	Code Red Internet Worm (CRv1, CRv2, and CRII)
3394	Microsoft IIS IDA/ISAPI Indexing Service Buffer Overflow

Affected
Affected Operating Systems

Operating System	Versions
Windows 95 [PATCH]	Any
Windows NT [PATCH]	4.0
Windows 98 [PATCH]	Any
Windows 2000 [PATCH]	Any
Windows NT Server [PATCH]	4.0
Windows Me [PATCH]	Any
Windows 2000 Server [PATCH]	Any

Affected Software and Programs

Software	Versions	Program	Versions
Internet Information Server (IIS) [PATCH]	4.0/5.0		
		Internet Explorer [PATCH]	5.01 SP1,5.5 SP1

Affected Services

Name	Type	Ports	RPC
HTTP	Web	80/TCP 8080/TCP	
SMB	Netbios	137/TCP 138/TCP 139/TCP 135/UDP 137/UDP 138/UDP 139/UDP	
TFTP	Data_transfer	69/UDP	

External Advisories

Advisory Name	Advisory Source
CA-2001-26 Nimda Worm>>Read	CERT
Nimda worm propagation>>Read	ISS
Mass Mailing Worm W32.Nimda.A@mm>>Read	National Infrastructure Protection Center
How to Protect Your Network Against the Nimda Virus>>Read	Cisco PSIRT

Links

General Information
General Information
General Information
Fix
Fix
Fix
General Information
General Information

Aliases

Vendor	Product	Alias
ISS	XForce	nimda-worm-propagation
XForce	Database	

FTP Authorization Failure

Siganture Id/Sub Id	6250/0
Signature Description	Triggers when a user has failed to authenticate three times in a row, while trying to establish an FTP session. This may be indicative of a brute force password guessing attempt, and may be viewed as an attempt to gain unauthorized access to system resources.
IDS Version	2.1.1
Alarm Level	2
Benign Triggers	Users that have forgotten passwords may trigger this signature.
Signature Type	NETWORK
Signature Structure	COMPOSITE
Implementation	CONTENT

Related Vulnerabilities

1003 Weak Passwords

Related T

TAC Case
TAC Case
TAC Case
Dynamic (

BUSINESS STRATEGIES & SOLUTIONS | NETWORKING SOLUTIONS & PROVISIONED SERVICES | P
TECHNOLOGIES | ORDERING | TECHNICAL SUPPORT | LEARNING & EVENTS | PARTNERS & RESEI
Home | Logged In | Profile | Contacts & Feedback | Site Help

Cisco Secure Encyclopedia

Quick Search: GO Advanced Search

FTP CWD ~root

General | Affected | Statistics | External

General

Key Attributes

Attributes/Severity	**High Severity**
Vulnerability Type:	Network
Exploit Type:	Access

Description
File Transfer Protocol (FTP) is one protocol by which files can be transferred to and from remote computer systems. The user transferring a file usually needs authority to login and access files on the remote system.

Some versions of FTP contain a vulnerability that allows the FTP daemon to reveal the full path of the home directory of the FTP user when the quote CWD command is used. By exploiting this vulnerability, an attacker can gain information about the structure FTP user's file system.

In particular, this vulnerability is present in versions of wuarchive ftpd predating April 8, 1993.

Consequences
An outside user can gather information about the FTP root directory, which can lead to further system access (including root access) and malicious activity.

Countermeasures
If the CWD command is enabled in your FTP server, refer to the server's documentation for information on how to disable the CWD command.

If you are running wuftp, upgrade to the most recent version, which is available at this URL: ftp://ftp.wustl.edu/packages/wuarchive-ftpd

Access

Access Required:	User or Anonymous
Access Gained:	root access

Products

IDS Signature FTP CWD ~root

SignatureId/ SubId	3152/0
CSID Versions:	2.1.1
Signature Description	Triggers when someone tries to execute the CWD ~root command. This may indicate an attempt to illegally access system resources.
Alarm Level	4
Benign Triggers	There is no known reason that this command should ever be executed.
Signature Type	NETWORK
Signature	

Structure	COMPOSITE
Implementation	CONTENT

IDS Signature FTP Improper Port Specified

SignatureId/ SubId	3154/0
CSID Versions:	2.1.1
Signature Description	Triggers if a port command is issued with a data port specified that is <1024 or >65535.
Alarm Level	4
Benign Triggers	No known triggers.
Signature Type	NETWORK
Signature Structure	ATOMIC
Implementation	CONTENT

Statistics

Statistical Data - for Hosts with FTP service enabled

Industry Vertical	Percentage of Hosts with this Vulnerability		Percentage of Hosts with Service Vulnerable	
Perspective	**Internal**	**External**	**Internal**	**External**
Advanced Technology				45.00%
Aerospace				57.14%
Photography				38.46%
Computers			27.91%	36.22%
Computers			33.11%	36.46%
Electronics/Chips			3.59%	33.33%
Software			21.66%	36.05%
Consumables			73.58%	
Food/Beverage			73.58%	
Financial Services			25.76%	4.33%
Banking			64.26%	31.58%
Finance			21.79%	3.73%
Insurance			36.67%	
Healthcare			60.46%	39.26%
Healthcare			63.92%	38.35%
Pharmaceuticals			60.26%	100.00%
Industrial			31.94%	37.04%
Building Materials			34.48%	100.00%
Construction			22.97%	
Farm Equipment				50.00%
Forest/Paper				20.00%
Industrial Equipment				40.00%
Internet			23.12%	
Internet/Web			23.12%	
Other			70.06%	29.63%
International			70.06%	
Unspecified				33.33%
Public Sector			38.53%	25.58%

Education		55.29%	54.55%
Government		37.08%	15.62%
Retail		49.51%	17.65%
Furniture		49.51%	17.65%
Service/Information	0.52%	28.57%	45.03%
Advertising		10.75%	
Media/Entertainment			44.57%
Outsource Services	16.67%	36.11%	66.67%
Services		58.70%	
Transportation		46.15%	
Motor Vehicles/Parts		100.00%	
Transportation		45.56%	
Utilities		20.73%	20.77%
Energy		21.38%	12.50%
ISP		47.22%	30.15%
Telco		20.47%	4.19%
Utilities		17.95%	
Overall	**0.09%**	**37.84%**	**21.59%**

.

Affected

Affected Operating Systems

Operating System	Versions
Generic Unix	Any

Affected Software and Programs

Software	Versions	Program	Versions
		wu-ftpd [PATCH]	Any

Affected Services

Name	Type	Ports	RPC
FTP	Data_transfer	20/TCP 21/TCP	

.

External Links

General Information
Fix
General Information
General Information

Aliases

Vendor	Product	Alias
Network Associates Inc.	Cybercop	FTPD QUOTE CWD ~ROOT BUG

Cisco Secure Encyclopedia

MSSQL xp_cmdshell Usage

Siganture Id/Sub Id	3732/0
Signature Description	This signature fires when an attempt to use the MSSQL 'xp_cmdshell' stored procedure is detected. This may represent an attempt to execute unauthorized commands on a MSSQL server.
IDS Version	S44
Alarm Level	0
Benign Triggers	The use of the 'xp_cmdshell' stored procedure may be normal system adminstration activity.
Signature Type	NETWORK
Signature Structure	COMPOSITE
Implementation	CONTENT

WWW PCCS MySQL Admin Access

Siganture Id/Sub Id	5079/0
Signature Description	The PCCS PHP-based MySQL administration tool contains a remotely accessible file which contains the databases administrator's username and password. This could be use to compromise the database.
IDS Version	2.2.1.6
CVE	CVE-2000-0707
Alarm Level	3
Benign Triggers	No known triggers.
Signature Type	NETWORK
Signature Structure	ATOMIC
Implementation	CONTENT

Related Vulnerabilities

2932 PCCS MySQL Administrator Password Exposure

TECHNICAL SUPPORT

Cisco Secure Encyclopedia

SNMP NT Info Retrieve

Siganture Id/Sub Id	4503/0
Signature Description	This signature detects an attempt to gain access to sensitive information about a Windows NT system. SubSigId 0 is fired when an attempt to enumerate the list of usernames is detected with SNMP OID .1.3.6.1.4.1.77.1.2.25. SubSigId 1 is fired when an attempt to enumerate the list of network shares is detected with SNMP OID .1.3.6.1.4.1.77.1.2.27. Other information available via SNMP includes the version of operating system, hostname, NT Domains, drives, and active services.
IDS Version	S3
Alarm Level	3
Benign Triggers	No known triggers.
Signature Type	NETWORK
Signature Structure	ATOMIC
Implementation	CONTENT

Related Vulnerabilities

3310 Microsoft SNMP Get Info

TECHNICAL SUPPORT

Cisco Secure Encyclopedia

SMB Authorization Failure

Siganture Id/Sub Id	6255/0
Signature Description	This alarm triggers when a client fails Windows NTs (or Sambas) user authentication three or more consecutive times within a single SMB session. This indicates that the user does not have a valid account name or password, the user has forgotten the password, or a password guessing attack like NAT is being used against the server. This alarm will also trigger on multiple failures to access a Windows 95 share. Share level access disregards the provided username and only uses the provided password.
IDS Version	2.1.1
Alarm Level	2
Benign Triggers	Users that have forgotten passwords may trigger this signature.
Signature Type	NETWORK
Signature Structure	COMPOSITE
Implementation	CONTENT

TECHNICAL SUPPORT

Cisco Secure Encyclopedia

Solaris in.fingerd Information Leak

Siganture Id/Sub Id	3456/0
Signature Description	This signature fires when an attempt to retrieve excessive information via the finger protocol is detected. SubSig 0: 'a b c d e f g h'@sunhost SubSig 1: 0@sunhost
IDS Version	S13
Alarm Level	3
Benign Triggers	No known triggers.
Signature Type	NETWORK
Signature Structure	ATOMIC
Implementation	CONTENT

Related Vulnerabilities

3592 Solaris in.fingerd Information Leak

TECHNICAL SUPPORT

Cisco Secure Encyclopedia

Unix Password File Access Attempt

Siganture Id/Sub Id	3201/0
Signature Description	These alarms triggers when any cgi-bin script attempts to retrieve password files on various operating systems. Such as the /etc/passwd (Sub ID 1), /etc/shadow (Sub ID 2), /etc/master.passwd (Sub ID 3), /etc/master.shadow (Sub ID 4), /etc/security/passwd (Sub ID 5), and /etc/security/opasswd (Sub ID 6). . This may indicate an attempt to illegally access system resources, in particular the /etc/passwd file. This may be the prelude to a more serious attack. No valid reason to access these files via this mechanism exists. Hosts that attempt to access the these files, especially from outside your network, should be shunned.
IDS Version	2.2.1.1
Alarm Level	4
Benign Triggers	No known triggers.
Signature Type	NETWORK
Signature Structure	COMPOSITE
Implementation	CONTENT

Related Vulnerabilities

1067 HTTP PHP View File

TECHNICAL SUPPORT
Cisco Secure Encyclopedia

TECHNICAL SUPPORT

Cisco Secure Encyclopedia

Linux Directory traceroute / nslookup Command Exec

Siganture Id/Sub Id	5255/0
Signature Description	This signature fires when an unauthorized attempt to execute commands using the CGI script "nslookup.pl" or "traceroute.pl" is detected.
IDS Version	S24
Alarm Level	4
Benign Triggers	No known triggers.
Signature Type	NETWORK
Signature Structure	COMPOSITE
Implementation	CONTENT

TECHNICAL SUPPORT

Cisco Secure Encyclopedia

Quick Search: GO Advanced Search

Toolkit: F

Feedback

Related T
TAC Case
TAC Case
TAC Case
Dynamic (

DNS Request for All Records

Siganture Id/Sub Id	6053/0
Signature Description	Triggers on a DNS request for all records. Similar to a zone transfer in that it provides a method for transferring DNS records from a server to another requesting host. The primary difference is that all DNS records are transferred not just those specific to a particular zone. This is indicative that your network may be under reconnaissance.
IDS Version	2.1.1
Alarm Level	2
Benign Triggers	This is a normal transaction on networks. If the source of the request was not a secondary server on your network this may be a reconnaissance effort, and heightened awareness of future security relevant events is suggested.
Signature Type	NETWORK
Signature Structure	ATOMIC
Implementation	CONTENT

Related Vulnerabilities

1133 DNS Reconnaissance Exploit

TECHNICAL SUPPORT

Cisco Secure Encyclopedia

Quick Search: GO Advanced Search

Toolkit: F

Feedback

Related T
TAC Case
TAC Case
TAC Case
Dynamic C

DNS Zone Transfer

Siganture Id/Sub Id	6051/0
Signature Description	Triggers on normal DNS zone transfers, in which the source port is 53. Zone transfers are the method by which secondary DNS servers update their DNS records. All DNS records are transferred at once from the primary to secondary server. This transfers records only for the zone specified. This is indicative that your network may be under reconnaissance.
IDS Version	2.1.1
Alarm Level	1
Benign Triggers	This is a normal transaction on networks. If the source of the request was not a secondary server on your network this may be a reconnaissance effort, and heightened awareness of future security relevant events is suggested.
Signature Type	NETWORK
Signature Structure	ATOMIC
Implementation	CONTENT

Related Vulnerabilities

1133 DNS Reconnaissance Exploit

ANEXO SERVIDOR PARA DETECÇÃO DE INTRUSOS
PARTE 3

COBRA Tecnologia S.A
Estrada dos Bandeirantes 7960
CEP 22783-110 Rio de Janeiro, RJ
Tel: 21 2442-3800
www.cobra.com.br

Administering the IDS MC Server

Administering the IDS MC server encompasses tasks associated with database rules, system configuration, and reports.

Caution User attempts to connect to the database directly can cause performance reductions and unexpected system behavior. It is strongly recommended that the user avoid attempting to connect to the database directly.

Using Database Rules

You can add, edit, view, and delete database rules. This section contains the following tasks:

Adding a Database Rule

You can use database rules to configure IDS MC to take an action at daily intervals or when a database threshold that you have defined is met. That action can be to send an e-mail notification, to log a console notification event, or to execute a script.

To add a database rule, follow these steps:

Step 1 Select **Admin > Database**.

The Database Rules page appears.

Step 2 Click **Add**.

The Specify Trigger Actions page appears.

Step 3 Specify the threshold to trigger Security Monitor to take an action. Then, click **Next**.

a. To trigger an action when the database exceeds a specified size, select the **Database used space greater than (megabytes)** check box. Then, specify the database size, in megabytes, that will trigger that action.

b. To trigger an action when the database free space is less than a specified size, select the **Database freespace less than (megabytes)** check box. Then, specify the database free space size, in megabytes, that will trigger that action.

c. To trigger an action when the total number of IDS events in the database exceeds a specified number, select the **Total IDS events** check box. Then, specify the number of IDS events that will trigger that action.

d. To trigger an action when the total number of SYSLOG events in the database exceeds a specified number, select the **Total SYSLOG events** check box. Then, specify the number of SYSLOG events that will trigger that action.

e. To trigger an action when the total number of events in the database exceeds a specified number, select the **Total events** check box. Then, specify the number of events that will trigger that action.

f. To trigger the action to occur daily, select the **Daily beginning** check box. Then, specify the date and time to start the action. The date is specified in month, day, and year format. The time is specified in hours, minutes, and seconds.

g. To enter a description for the Database Rule, enter a description in the Comment field.

The Choose the Actions page appears.

Step 4 Specify the action for IDS MC to take when the threshold specified in Step 3 is met. You can select more than one action.

a. To send an e-mail notification when the specified threshold is met, select the **Notify via Email** check box. Then, enter the e-mail address for the recipient(s) in the Recipient(s) field. If you enter more than one e-mail address, separate the addresses with commas. Enter the subject for the message in the Subject field and the message body text in the Message field. You can use the keyword substitutions listed in Table 8-1 in the Subject and Message fields:

Table 8-1 Keyword Substitutions

Keyword	Description
${RuleName}	The name of the event rule.
${RuleDescr}	The description of the event rule.
${Filter}	The query filter for the event rule.
${Interval}	The query interval for the event rule.
${Initial}	The initial threshold for the event rule.
${Repeat}	The repeat threshold for the event rule.
${DateStr}	Date stamp for when the event rule was triggered, based on the server-local time. The datestamp appears in YYYY/MM/DD format.
${TimeStr}	Time stamp for when the event rule was triggered, based on the server-local time. The timestamp appears in HH:MM:SS TZ format, where HH is in 24-hour form.
${GmtDateStr}	The Greenwich Mean Time (GMT) date stamp for when the rule was triggered in YYY/MM/DD format.
${GmtTimeStr}	GMT time stamp for when the event rule was triggered in HH:MM:SS TZ format, where HH is in 24-hour form and TZ is always UTC.
${MsgCount}	The number of matches that occurred in the current interval causing this rule to be triggered.

Table 8-1 Keyword Substitutions (continued)

Keyword	Description
${Threshold}	The threshold that was met, causing the event rule to be triggered. This value will be the same as either **${Initial}** or **${Repeat}**.

Note The keyword matching (inside the brackets) is case-insensitive.

b. To log a console notification to the audit log when the specified threshold is met, select **Log a Console Notification Event** check box. Then, enter your user name in the User Name field. Select an alarm event level from the Severity list box and enter a message in the Message field. You can use the keyword substitutions listed in Table 8-1.

Tip To view the console notification messages, run the Console Notification Report on the Reports > Generate page.

c. To execute a script when the specified threshold is met, select **Execute a Script** check box. Then, select a script from the Script File list box. You can enter any required arguments in the Arguments field.

Note The scripts included with IDS MC are for database pruning and are more applicable for database rules than for event rules. However, you can add your own custom scripts to the list. For more information, see Learn More About Executing a Script from a Database or Event Rule, page 8-5.

Tip You can use the keyword substitutions listed in Table 8-1 in the Arguments field. If you use one of these keyword substitutions, surround the keyword with quotation marks. For example, you might use **"${RuleDescr}"** as an argument.

Step 5 Click **Finish**.

The Database Rule is added.

Learn More About Executing a Script from a Database or Event Rule

One of the actions you can select from the Choose the Actions page is Execute a Script. If you select **Execute a Script**, you must select a script from the **Script File** list box.

IDS MC provides the following scripts:

- **PruneByAge.pl**--Prunes alarms older than the specified number of days from the specified tables. Use as follows:

  PruneByAge.pl age "tablelist"

  - **age**—Specifies the number of days. The default value is 20.
  - **tablelist**—Specifies the type of table to be pruned. You can list more than one table in a comma-delimited list. You can choose from the following table types:
  - **syslog**—SYSLOG event table
  - **alert**—Alert table
  - **auditlog**—Audit log table
  - **deploy**—Deployment jobs table
  - **sysconfig**—System configuration table

    The default value is all tables ("syslog,alert,auditlog,deploy,sysconfig").

- **PruneByDate.pl**--Prunes alarms from the specified tables generated on and before the specified date. Use as follows:

  PruneByDate.pl "date" "tablelist"

  - **date (Required)**—Specifies the date to delete alarms on and before. The date format is "MM/DD/YYYY,HH:MM".
  - **tablelist**—Specifies the type of table to be pruned. You can list more than one table in a comma-delimited list. You can choose from the following table types:
  - **syslog**—SYSLOG event table
  - **alert**—Alert table
  - **auditlog**—Audit log table

- **deploy**—Deployment jobs table
- **sysconfig**—System configuration table

The default value is all tables ("syslog,alert,auditlog,deploy,sysconfig").

- **PruneBySeverity.pl--**Prunes alarms of the specified severity from the specified tables. This script is order-specific: You must specify the severity before you specify the table list. Use as follows:

  PruneBySeverity.pl "severitylist" "tablelist"

  - **severitylist**—Specifies the severity level of the alarms to prune. You can choose from the following severity levels.
  - **h**—High severity
  - **m**—Medium severity
  - **l**—Low severity
  - **i**—Informational severity

    The default value is "i,l,m".
  - **tablelist**—Specifies the type of table to be pruned. You can list more than one table in a comma-delimited list. You can choose from the following table types:
  - **syslog**—SYSLOG event table
  - **alert**—Alert table
  - **auditlog**—Audit log table

    The default value is all tables ("syslog,alert,auditlog").
- **PruneMarkedForDeletion.pl--**Prunes alarms already marked for deletion from the specified tables. Use as follows:

  PruneMarkedForDeletion.pl "tablelist"

  - **tablelist**—Specifies the type of table to be pruned. You can list more than one table in a comma-delimited list. You can choose from the following table types:
  - **syslog**—SYSLOG event table
  - **alert**—Alert table
  - **auditlog**—Audit log table

    The default value is all tables ("syslog,alert,auditlog").

- **PruneSpecifyCmdLine.plxd1** Prunes alarms from the specified tables using the specified alarms. Use as follows:

  PruneSpecifyCmdLine.pl -r"tablelist" [-p] [-t"date"] [-a#] [-s"severities"] [-w"dirname"]

  - **-r"tablelist" (Required)**—Specifies the type of table to be pruned. You can list more than one table in a comma-delimited list. You can choose from the following table types:
  - **syslog**—SYSLOG event table
  - **alert**—Alert table
  - **auditlog**—Audit log table
  - **deploy**—Deployment jobs table
  - **sysconfig**—System configuration table

    For example, **-r"alert,syslog"**.
  - **-p (Optional)**—Prunes all records already marked for deletion in the specified table. By default, alarm records are not pruned from the database.
  - **-t"date" (Optional)**—Prunes all records that are older that the specified date from the specified table. The date format is "MM/DD/YYYY,HH:MM".

    Note You cannot use -t"date" and -a# in the same argument.
  - **-a# (Optional)**—Prunes all records that are older than the specified number of days from the database, where # is a positive integer representing the number of days.

    Note You cannot use -t"date" and -a# in the same argument.
  - **-s"severity" (Optional)**—Prunes all records with the specified severity from the specified table. You can list more than one severity in a comma-delimited list.
  - **h**—High severity
  - **m**—Medium severity

- **l**—Low severity
- **i**—Informational severity

  For example, **-s"i,l,m"**.
- **-w"dirname" (Optional)**—Outputs comma-delimited files to the specified directory. There is one file output for each table specified.

Additionally, you can add your own custom scripts. To add a custom script, place your script file in the *X*:/Program Files/CSCOpx/MDC/etc/ids/scripts folder, where *X* is the drive where IDS MC is installed. If you add your script to this folder, it will appear in the Script File list box.

Caution IDS MC cannot verify that scripts are valid or that they will execute as expected. A poorly written custom script can cause your system to fail.

Editing a Database Rule

Editing a database rule is similar to creating a database rule. The edit database rule wizard takes you through the same panels that you used to create the database rule.

To edit a device configuration, follow these steps:

Step 1 Select **Admin > Database**.

The Database Rules page appears.

Step 2 Select the radio button corresponding to the database rule that you want to edit, and then click **Edit**.

The Specify the Trigger Conditions page appears.

Step 3 Make any necessary changes to the fields that you want to revise. Click **Next** to access the Choose the Actions page to make changes.

Step 4 To save your changes, click **Finish**.

Step 5 To edit another database rule, repeat Step 2 through Step 4.

Viewing Database Rule Details

This procedure provides the basic steps for viewing detail information for a database rule. You cannot edit database rules from the View Database Rule page.

To view a database rule, follow these steps:

Step 1 Select **Admin Database Rules**.

The Database Rules page appears.

Step 2 Click the radio button next to the database rule that you want to view.

Step 3 Click **View**.

The View Database Rule page appears. Detailed information about the rule appears in the View Database Rule text box.

Step 4 Click **OK** to return to the Database Rules page.

Deleting a Database Rule

You can delete database rules that you no longer want to use.

To delete a database rule, follow these steps:

Step 1 Select **Admin > Database**.

The Database Rules page appears.

Step 2 Select the radio button corresponding to the database rule that you want to delete.

Step 3 Click **Delete**.

The database rule is deleted from IDS MC.

Updating Sensor Software

To query your sensors and update their software if necessary, follow this procedure:

Updating IDS Sensor Software Versions and Signature Release Levels, page 5-59

Updating Signatures

To learn whether Cisco Systems has released one of its periodic updates of signatures for IDS MC, follow this procedure:

Updating IDS Sensor Software Versions and Signature Release Levels, page 5-59

Defining the E-mail Server Settings

You can specify the e-mail server that IDS MC uses for event notifications.

To define the e-mail server settings, follow these steps:

Step 1 Select **Admin > System Configuration**.

Step 2 Click **E-mail Server** in the TOC.

The E-mail Server page appears.

Step 3 Enter your e-mail server name in the Server Name box.

Step 4 To save your changes, click **Apply**.

The e-mail server you specify will be used to send event notifications.

Approving Configuration Files

You can configure IDS MC to automatically or manually approve configuration files when they are generated. The default value is automatic approval.

You must have a user account with adequate privileges to approve configuration files.

To automatically approve configuration files when they are generated, follow these steps:

Step 1 Select **Admin > System Configuration**.

Step 2 In the TOC, select **Configuration File Management**.

Reports

The Reports tab is where you can generate and view audit log reports about network activities monitored by sensors on your network.

When you generate a report, you can run it immediately or you can schedule it to run at a later time. Scheduled reports can be run once or repeatedly.

For step-by-step procedures on performing a specific task, refer to the corresponding section.

- Scheduling and Generating Reports, page 8-13
- Viewing Reports, page 8-15
- Deleting Scheduled Report Templates, page 8-18
- Saving a Generated Report as an HTML File, page 8-15
- Deleting Generated Reports, page 8-16
- Editing Report Parameters, page 8-17

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.
- **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.

To generate a report, follow these steps:

Step 1 Select **Reports > Generate**.

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**.

The Report Filtering page appears.

Step 3 Enter the report parameters for the report type you selected. Then, click **Next**.

The Schedule Report page appears.

Step 4 Enter a name for the report in the Report Title field.

Step 5 To export the generated report to an HTML file, select the **Export to** check box. Then, specify the exact path to the file that is to contain the generated report. The path should include the filename and the desired extension; for example, **/<dir>[/<dir>/[...]]/<filename>[.<ext>]**. No extension is appended to the filename if you do not specify an extension.

Step 6 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 7 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**.

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.

About Viewing Reports

When you select **Reports** > **View**, the Choose Completed Report page appears. From that page, you can view generated reports. You also can export reports to HTML files and delete unwanted reports. If the report was generated from a scheduled report template, deleting the report does not delete the associated scheduled report template.

This section contains the following procedures:

Viewing Reports

After you generate a report, you can view it.

Tip To understand how data is sorted in a report, refer to the numbers that appear in the column headings of the generated report. These numbers represent the sort keys. For example, data is sorted first based on the data in the column with a (1) in it, followed by the data in the column with a (2) in it, and so on.

To view a report, follow these steps:

Step 1 Select **Reports > View**.

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**.

The report appears in the Report page.

Step 4 To view the report in a new browser window, click **Open in Window. . ..**

The report appears in a new browser window.

Saving a Generated Report as an HTML File

After you generate a report, you can save the report as an HTML file.

To save a generated report as an HTML file, follow these steps:

Step 1 Select **Reports > View**.

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 To select the report that you want to export, select the check box corresponding to the report title.

Step 3 Click **Open in Window**.

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**.

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**.

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**.

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 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.

A check mark appears next to each report you selected.

Step 3 To delete the selected report, click **Delete**.

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**.

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.

A check mark appears next to the report you selected.

Step 3 To open the selected report template, click **Edit**.

A new page displays the report parameters. Depending on the type of report, the parameters are different.

Step 4 Change any report parameters that you want to. To save your changes, click **Finish**.

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**.

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.

A check mark appears next to each report you selected.

Step 3 To delete the report template, click **Delete**.

The selected report template and all associated end reports are deleted.

Using the Event Viewer

You can use Event Viewer to view real-time and historical events. Events include IDS alerts (generated by network-based and host-based sensors, IOS devices, and PIX Firewalls), syslog messages, and audit logs. This section contains the following topics:

Understanding Event Viewer Basics and Settings

Sensors and other network devices can continually forward events to Monitoring Center for Security (Security Monitor). These events are stored in the Security Monitor database. Event Viewer allows you to view the events stored in the Security Monitor database. You can view real-time events as they are forwarded to Security Monitor, and you can also view historical events stored in the database.

Note Event Viewer is not the same as the Windows Administrative Tool also known as Event Viewer.

The following list contains examples of events that can be viewed in Event Viewer:

- An attempt to break into a computer (IDS Alerts)
- General security-related messages (Security Summaries)
- A status message from a program or a computer (Audit Logs)

Event Viewer queries the database at regular intervals to extract the most recent events.

To learn more about Event Viewer, see the following topics:

Event Display

Event Viewer combines the functionality of a spreadsheet (such as Lotus 1-2-3 or Microsoft Excel) with that of a hierarchical, drill-down directory (such as Windows Explorer) to create a collection of event records called a *drillsheet* (a *drill*down spread*sheet*). The drillsheet displays groups of similar event records on a single row of a grid, enabling you to detect patterns in the data.

Event Viewer contains a grid pane that organizes and displays event records. Event Viewer can read real-time events and historical events from the database. You can configure the grid pane in a variety of ways to display information about alarms detected by the sensor. For example, you can delete unwanted columns and expand and collapse cells.

A drillsheet has rows and columns, and the intersection of a row and a column is called a *cell*.

The background color of a cell gives some information about the cell:

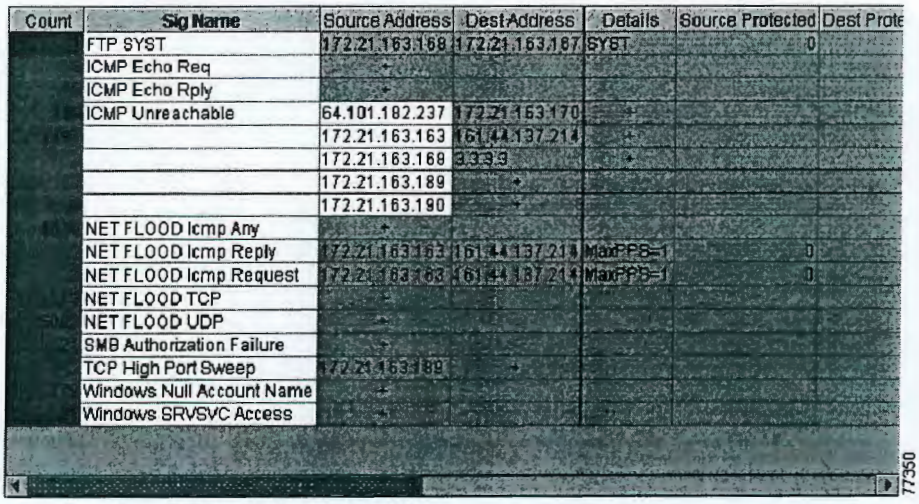
- If a cell is white, only one data element is associated with that cell.
- If a cell is gray, that cell may represent more than one data element.
  - If a cell is gray and displays the + symbol, that cell represents more than one data element. You can see all the data elements by double-clicking this cell.
  - If a cell is gray but displays a single data element (for example, 172.21.172.6), that cell has not been expanded, but it contains only a single data element, so that element is displayed anyway.

Note You can use the Preferences panel to modify the Event Viewer behavior.

Note The conventions governing the background colors of cells in the Count column are different and are described in Status Propagation, page 4-7.

For example, in Figure 4-1, there is more than one source address associated with the events that have the name "ICMP Echo Req". Therefore, the Source Address cell in the ICMP echo request row is gray and displays "+". We also see that Source Address column has been expanded for the "ICMP Unreachable" events. Therefore, the cells in the Source Address column for the ICMP Unreachable rows are white. Finally, note that the destination address 172.21.163.170 has a gray background but has data displayed, rather than a "+". This means that this cell has not been expanded, but there is only one data element to be displayed, so it is displayed anyway.

Figure 4-1 Event Viewer Drillsheet



Count	Sig Name	Source Address	Dest Address	Details	Source Protected	Dest Prote
	FTP SYST	172.21.163.168	172.21.163.187	SYST	0	
	ICMP Echo Req	+				
	ICMP Echo Rply	+				
	ICMP Unreachable	64.101.182.237	172.21.163.170	+		
		172.21.163.163	161.44.137.214	+		
		172.21.163.168	3.3.3.3	+		
		172.21.163.189	+			
		172.21.163.190	+			
	NET FLOOD Icmp Any	+				
	NET FLOOD Icmp Reply	172.21.163.163	161.44.137.214	MaxPPS=1	0	
	NET FLOOD Icmp Request	172.21.163.163	161.44.137.214	MaxPPS=1	0	
	NET FLOOD TCP	+				
	NET FLOOD UDP	+				
	SMB Authorization Failure	+				
	TCP High Port Sweep	172.21.163.189	+			
	Windows Null Account Name	+				
	Windows SRVSVC Access	+				

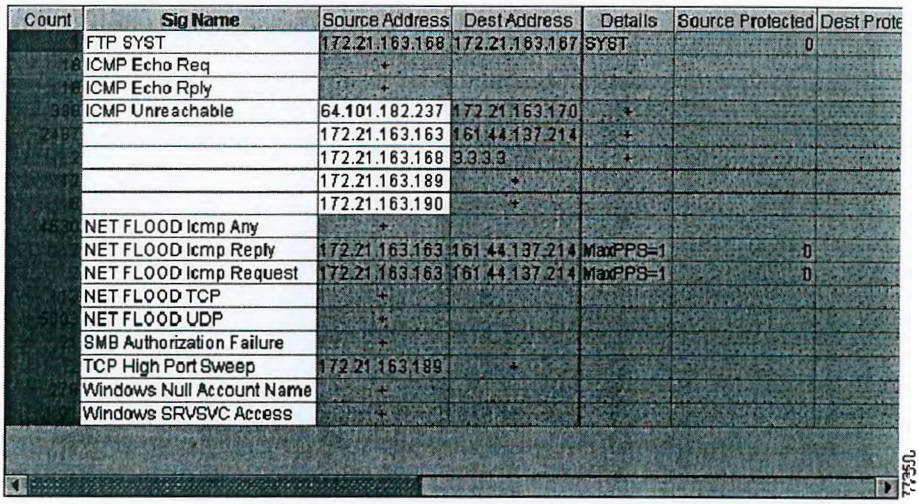
77350

Selecting Cells

Many of the functions performed by Event Viewer require you to select cells in the drillsheet. Typically, you select a cell by clicking it. It is important to understand what it means to select a cell in the drillsheet.

When you select a cell in the drillsheet you are actually selecting a node in the event tree. When you perform an operation against a selected cell, you are actually performing an operation on all branches of nodes that pass through the selected cell. For example, in Figure 4-2, if you select the "ICMP Unreachable" cell, any operation that you run on that cell is performed for all events that have the name "ICMP Unreachable." In this case, that would be all elements in rows 4 through 8. If you intend to execute an operation against only row 4, you must select, in Figure 4-2, either the "64.101.182.237" cell or a cell to its right.

Figure 4-2 Event Viewer Drillsheet



Count	Sig Name	Source Address	Dest Address	Details	Source Protected	Dest Prote
	FTP SYST	172.21.163.168	172.21.163.167	SYST	0	
18	ICMP Echo Req	+				
18	ICMP Echo Rply	+				
388	ICMP Unreachable	64.101.182.237	172.21.163.170	+		
2487		172.21.163.163	161.44.137.214	+		
		172.21.163.168	3.3.3.3	+		
72		172.21.163.189	+			
6		172.21.163.190	+			
4530	NET FLOOD Icmp Any	+				
	NET FLOOD Icmp Reply	172.21.163.163	161.44.137.214	MaxPPS=1	0	
	NET FLOOD Icmp Request	172.21.163.163	161.44.137.214	MaxPPS=1	0	
41	NET FLOOD TCP	+				
5803	NET FLOOD UDP	+				
	SMB Authorization Failure	+				
	TCP High Port Sweep	172.21.163.189	+			
928	Windows Null Account Name	+				
	Windows SRVSVC Access	+				

77350

Furthermore, if you select a cell that is blank because its value is implied by the cell above it (for example, the cell just below the "ICMP Unreachable" cell), the branch of the node that is operated on is the branch that is defined by the first cell that is filled in to the right of the blank cell that you selected. For example, in Figure 4-2, if you select the blank cell just below the "ICMP Unreachable" cell, when you perform an action, Event Viewer behaves as though you selected the "172.21.163.163" cell.

Note You can use the Preferences panel to change this behavior. For more information, see Specifying Event Viewer Preferences, page 4-21.

The Count Column and the Event Count Tool-Tip

Event Viewer provides two mechanisms for displaying the number of events in a group: the Count column and the event count tool-tip.

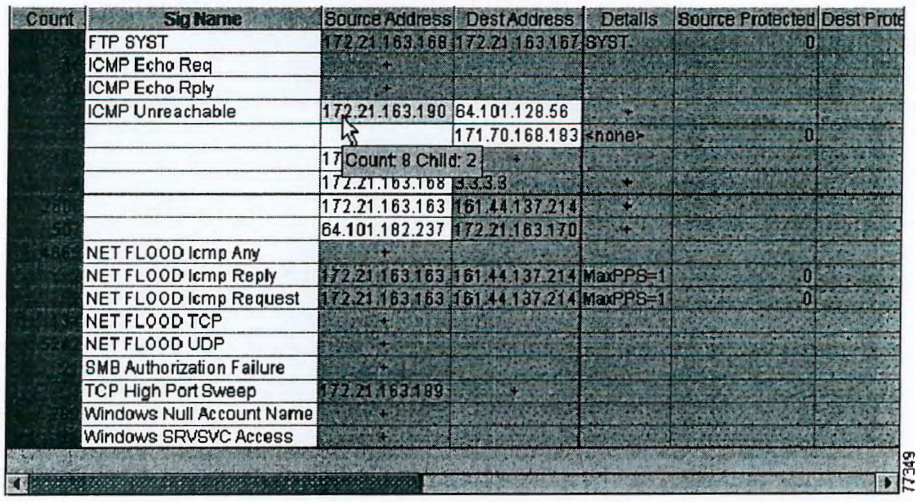
- **Count Column**—The Count column is the first column in the drillsheet; you cannot move, collapse, or delete it. In the Count column, a cell for a given row displays the number of events represented by that row. For example, the drillsheet in Figure 4-3 indicates that there are 18 "ICMP Echo Req" events.

However, the count of 7 in the fourth row does not mean that there are 7 "ICMP Unreachable" events; it means that there are 7 "ICMP unreachable" events with a source address of "172.21.163.190" and a destination address of "64.101.28.56".

- **Event Count Tool-Tip**—You can find out how many events are represented in a branch that spans more than one row by resting the mouse pointer on the cell you are interested in. A tool-tip indicates how many events pass through that branch. The tool-tip also displays a *child count*. The child count is the number of unique data elements to the right of the cell you have selected.

In Figure 4-3, when you rest the mouse pointer on the source address 172.21.163.190, you see a count of 8 and a child count of 2. This means that there are 8 "ICMP Unreachable" events with a source address of 172.21.163.190. The values in the Count column confirm this. The Count column indicates that there are 7 events with the fields "ICMP Unreachable," 172.21.163.190 and 64.101.128.56 and 1 event with the fields "ICMP Unreachable," 172.21.163.190 and 171.70.168.183. The sum of 7 and 1 is 8.

Figure 4-3 Event Count Tool-Tip



Status Propagation

This section describes how Event Viewer determines the severity for individual events and groups of events.

- **Individual Events**—Some events are more severe than others. Some events represent unmistakable and devastating actions, while others might represent occurrences that are either less damaging or more ambiguous, or both. To indicate the severity of an alarm, a sensor associates a severity level with each alarm that is generated. In general, those severity levels are Informational, Low, Medium, and High, and the colors associated with those levels are blue, green, yellow, and red, respectively.
- **Event Groups**—Event Viewer uses a "propagate most severe" status propagation scheme. This means that in a group of events, the severity of the group is the severity of the most severe event in the group. For example, if an event group contains one *High* event and 17 *Low* events, the severity of the group is *High*.

  The background color of the event group's Count column cell is the color associated with the event group's severity. For example, if row number 17 represents 200 events, and if one of those 200 events is High, the event group itself is considered High, and the background color of the Count column cell at row number 17 is red.

Note You can modify the Event Viewer preferences to use icons instead of color to indicate status.

The status of the rows is modified in real time when events are added or deleted or when you manipulate the rows.

In addition to being shown in the Count column, the severity of an event group is reflected in the Severity column. For more information about how you can manipulate drillsheets to group events by severity, see Sorting Data and Shifting Columns, page 4-9.

Context Buffer

Some alarms have *context buffers* associated with them. Context buffers record exactly what traffic was traversing the network at the time the alarm's signature was detected. The context buffer contains up to 256 bytes of incoming traffic and 256 bytes of outgoing traffic.

Not all events have context buffers. The following is a partial list of alarms that have context buffers:

- 3100 Smail Attack
- 3101 Sendmail Invalid Recipient
- 3102 Sendmail Invalid Sender
- 3103 Sendmail Reconnaissance
- 3104 Archaic Sendmail Attacks
- 3200 WWW Phf Attack
- 3201 WWW General cgi-bin Attack
- 6251 Telnet Authorization Failure
- 8000 String Match

  The 8000 signature contains the following subsignatures:

  - 2101 FTP Retrieve Password File
  - 2302 Telnet-/etc/shadow Match
  - 2303 Telnet-++
  - 51301 Rlogin-IFS Match
  - 51302 Rlogin-/etc/shadow Match
  - 51303 Rlogin-++

For more information about signatures, see the Network Security Database (NSDB). You can access the NSDB at https://*hostname*/vms/nsdb/html/all_sigs_index.html, where *hostname* is the name of the computer on which Security Monitor is installed. For information about viewing the NSDB entry for an event in Event Viewer, see Learning About Attacks, page 4-25.

If even one event represented by a row has a context buffer, the value in the Count column is **bold**. To view the context buffer(s) associated with an event group, select a cell, and then select **View > Context Buffer** in the TOC. For more information, see Viewing the Context Buffer, page 4-23.

Sorting Data and Shifting Columns

You can sort data within a column and you can change the order of columns to help you find data.

Sorting Data

By default, all columns except time-related columns and Severity columns are displayed in ascending order. This means that, from top to bottom, numbers are displayed from least to greatest, and words are displayed from A to Z. To change the sorting scheme of a column from ascending to descending (or vice versa), click the column header. To change it back, click the column header again.

Note By default, time-related columns (times, dates, and timestamps) are displayed in descending order. The most recent dates are displayed at the top of the list, ensuring that recent events are displayed at the top of lists. To change to ascending order, click the column header. By default, Severity columns are displayed in ascending order on the basis of priority (Info, Low, High). To change to descending order (High, Low, Info), click the column header.

Sorting within a drillsheet is different from sorting in a spreadsheet in one significant way: In a drillsheet, sorting data elements in a particular column is constrained by the nature of the data in the columns to the left.

For example, Table 4-1 shows two columns. The first column has last names, and the second column has first names.

Table 4-1 First Names Sorted in Ascending Order

Last Name	First Name
Baker	Alan
	Wanda
Jones	Bob

Table 4-1 First Names Sorted in Ascending Order (continued)

Last Name	First Name
	Xena
Smith	Charles
	Yvonne

The Last Name column and the First Name column are ascending. First names are associated with last names, so any sorting of first names must be within last names. If you click the First Name header to change the sorting scheme to descending, you obtain the results shown in Table 4-2.

Table 4-2 First Names Sorted in Descending Order

Last Name	First Name
Baker	Wanda
	Alan
Jones	Xena
	Bob
Smith	Yvonne
	Charles

The data in the first column did not change when you changed the sorting scheme of the second column.

Shifting Columns

The order of the columns in a drillsheet determines how events are grouped together. For example, if your first three columns (excluding the Count column) are, in order, Name, Source Address, Dest Address, all events are grouped by name, and then each of those name groups is divided into subgroups by source address, and then each of those subgroups is divided into even smaller groups by destination address.

To change the way events are grouped, you must change the order of the columns.

To change column order, click and hold the cursor over the header of the column you want to move, and then drag the header to the desired location and release the mouse button. The window is redrawn.

Note In Security Monitor versions earlier than 1.2, changes in column order are not persistent: If you close and re-open a drillsheet, the columns appear in their original order.

In most cases, redrawing after a column shift is nearly instantaneous. However, with large numbers of events (tens of thousands or more), a slight delay may occur during redrawing.

The Count column is always the first column in the display. You cannot drag the Count column to another position, and you cannot drag another column to the left of the Count column. If you attempt to move the Count column the columns revert to their original positions.

When columns are shifted, the entire window is redrawn, meaning that all rows are expanded to the Event Expansion Boundary for that window. To reduce the number of rows that are drawn with each column shift, consider making one of the first few columns the Event Expansion Boundary.

Graphing Features

You can display Event Viewer data as a bar graph. Two types of graph are available:

- Graph > By Child
- Graph > By Time

Each bar in the graph depicts two things:

- The total number of events represented by the bar
- The breakdown of events by severity for the events represented by the bar

The event count is denoted by the y-axis. The severity breakdown is depicted in each bar as a "stack" of colors, where blue, green, yellow, and red represent Info, Low, Medium, and High severity, respectively.

You can select which events in the viewer are graphed. You can also specify how the events are graphed; in other words, you can specify the field that defines the x-axis grouping. Each is described below.

- **Selecting the subset of events to graph**—In the Event Viewer "grid" display, select the node (cell) that corresponds to the events you want to graph. If you want a graph of all events in the viewer, select the top-left cell in the display (the root node).
- **Selecting the way in which events are grouped (x-axis)**—You can select how events are grouped on the x-axis in several ways.

  If you want to see how the selected events were distributed over time, select **Graph > By Time**.

  If you want to group events by some field in the display, select **Graph > By Child**. The "Child" means that for a selected node in Event Viewer, a graph will be drawn in which the x-axis is defined by the selected node's "child" nodes, that is, the nodes in the column to the right of the selected node. For example:

  Let's say that you are viewing All IDS Events in your Event Viewer, and you would like to see a graph that breaks down the events by attack type (denial of service, reconnaissance, worms, and so on) for just IDIOM (4.0 and later) Sensors.

  To do this, drag and drop the **IDS Alarm Type** column just to the right of the Count column, and then drag the **Attack Type** column just to the right of the IDS Alarm Type column. Now, select the cell in the IDS Alarm Type column that says IDS IDIOM, and then select **Graph > By Child**.

  You will see a graph of all IDIOM (4.0 and beyond Sensor) events, grouped by attack type. For each bar, which represents a particular attack type, you will see the total number of events (represented by the height of the bar) and the breakdown by severity (represented by the height of the colors within the bar).

Deleting Columns

You can delete a column from the Event Viewer display. Deleting a column affects only the Event Viewer display that you are viewing. It does not change the default column arrangement for other existing or future Event Viewer displays.

To delete a column from the current Event Viewer display, select any cell in the column that you want to delete. Then, select **Edit > Delete > Column**.

Starting Event Viewer

Before you start Event Viewer, you must specify which events you want to display.

Note Event start and stop times are the times at which events were stored in the database, not the time that the events were generated by the sensor. Usually, the two times are close, if not identical. Storage and generation times differ greatly only if there are communications problems that postpone sending events from the sensor to the database.

To start Event Viewer, follow these steps:

Step 1 Select **Monitor > Events**.

The Launch Event Viewer page appears.

Step 2 To select which event type appears in Event Viewer, select an option from the **Event Type** list box.

Step 3 Select an option from the Column Set list box:

- **Last Saved**—If you choose **Last Saved**, Security Monitor queries the database to retrieve your customized set of columns.
- **Default**—If you choose **Default**, Security Monitor provides the set of columns provided with Version 1.1 and earlier.
- **All**—If you choose **All**, Security Monitor provides all possible columns—the recommended columns and then all the remaining columns.

Step 4 Select an option in the **Event Start Time** section to specify the oldest events that appear in Event Viewer.

- Select **At Earliest** to view events starting with the oldest stored in the database.
- Select **At Time** to specify a date and time from which you want to start displaying events.

Step 5 Select an option in the **Event Stop Time** section to specify the most recent events that appear in Event Viewer.

- Select **Don't Stop** for real-time event analysis.
- Select **At Time** to specify a date and time up to which you want to display events.

Step 6 To start Event Viewer, click **Launch Event Viewer**.

Event Viewer appears.

Tip To start another Event Viewer window from the current Event Viewer window, select **File > New > Window** in Windows Explorer or **File > New > Navigator Window** in Netscape Navigator.

Working in Event Viewer

This section describes the tasks that you can perform from the menus in Event Viewer.

Deleting an Event from the Event Viewer Display

You can delete an event or set of events from the current Event Viewer display without removing these events from the database or other, concurrently running Event Viewers.

To delete an event from the current Event Viewer display, follow these steps:

Step 1 Select a cell in the Event Viewer display.

Step 2 Select **Edit > Delete > From this Grid**.

The Event Viewer display appears again, reflecting the deletion of the cell that you selected.

Deleting a Column from the Event Viewer Display

You can delete a column from the current Event Viewer display. Deleting a column from the current Event Viewer display does not delete the events in that column from the database, nor does it mark the events in that column for deletion from the database.

To delete a column from the current Event Viewer display, follow these steps:

Step 1 Select any cell in the column that you want to delete.

Note You cannot delete the Count column.

Step 2 Select **Edit > Delete > Column**.

The Event Viewer display appears again, reflecting the deletion of the column that you selected.

Deleting Events from the Database Manually

You can delete events from the database manually when you no longer need those events or when you want to reduce the size of the database.

Deleting events manually involves executing a script at a command prompt. Other methods of deleting events involve using database rules, event rules, or Event Viewer.

Note Because of the way alarm data is stored in the database, there will not always be a one-to-one correspondence between the number of events deleted from the event display and number of records removed from the relational database.

Deleting events manually is the best method for deleting events that you no longer need. Manual deletion also is the best method to use when your database has grown larger than you want. Database rules and event rules can help you maintain the content and size of your database, but they are not as effective when you need to delete events; because you have to wait for rules to be triggered. Deleting events through Event Viewer is best only when the number of events in the database is less than 1,000,000.

To use this procedure, you must have access to the Security Monitor server. If you do not, you cannot execute a script in a command window.

To delete events from the database,

Step 1 Choose a script that is suited to the reason that you want to delete events:

- **PruneByAge.pl**—Choose this script when you want to delete events that are older than a specific number of days.
- **PruneByDate.pl**—Choose this script when you want to delete events that occurred on or before a specific date.

- **PruneBySeverity.pl**—Choose this script when you want to delete events because your database contains low-severity events that you do not need to keep.
- **PruneDefault.pl**—Choose this script when you want to delete events because your database has too many events (because your database is too big).
- **PruneSpecifyCmdLine.pl**—Choose this script when you want to delete events by specifying alarms.

Tip The available scripts are stored on the Security Monitor server in `~CSCOpx/MDC/etc/ids/scripts`.

Step 2 Open a command window and execute the script that you have chosen.

The script will run in a separate thread, so you can continue working with Security Monitor.

Step 3 If your database has less than 1,000,000 events, you can delete those events through Event Viewer:

a. To delete events through Event Viewer *if your database has less than 1,000,000*, select one or more cells in Event Viewer.

b. Select **Edit > Delete > From Database**.

c. Execute the PruneMarkedForDeletion.pl script or the Alarm Export Utility.

Collapsing Cells

When a cell is collapsed, all branches that pass through the selected cell provide less detail. For each branch, the background color of the cells in the newly hidden column changes from white to gray. Also, rows are removed as necessary to conceal the appropriate data.

Note Collapsing does not delete anything; it merely hides data from view.

Events can be collapsed by one column, by first group, or all the way (all columns). If a cell is collapsed by one column, each branch through the selected cell gives one less column of detail. If a cell is collapsed by first group, Event Viewer traverses the tree from the selected node and collapses all nodes up the branch until a node with multiple child nodes is collapsed. If a cell is collapsed all the way, all branches through the selected cell are condensed into the selected cell.

To collapse a cell, follow these steps:

Step 1 Select a cell in Event Viewer.

The selected cell is highlighted and outlined in gray.

Step 2 To collapse a cell by one column, select **Edit > Collapse > One Column**.

Step 3 To collapse a cell by first group, select **Edit > Collapse > First Group**.

Step 4 To collapse a cell all the way, select **Edit > Collapse > All Columns**.

Setting the Event Expansion Boundary

The Event Expansion Boundary dictates the number of a new event's columns that will be expanded if the new event does not match an existing event group. The cells in an event are expanded as long as the event matches an existing event group. After there are no matches, a new row is created for the event, and the cells in the new event are expanded until the Event Expansion Boundary is reached.

The default value for the Event Expansion Boundary is one column. You can change the default value in the Preferences dialog box.

To set the Event Expansion Boundary, follow these steps:

Step 1 To establish a column as the Event Expansion Boundary, select a cell in that column.

The selected cell is highlighted and outlined in gray.

Step 2 Select **Edit > Set Event Expansion Boundary**.

The Event Expansion Boundary is set. The column heading is bold.

Expanding Cells

When a cell is expanded, all *branches* that pass through the selected cell provide more detail. For each branch, the background color of the cells in the newly filled-in column(s) changes from gray to white. Also, rows are created as necessary to display the exposed data.

Event rows can be expanded by one column, by first group, and by all columns. If a cell is expanded by one column, each branch through the selected cell gives one more column of detail. If a cell is expanded by first group, Event Viewer traverses the tree from the selected node and expands all nodes down the branch until a node with multiple children is reached. If a cell is expanded all the way, all branches through the selected cell are fully expanded.

Note Sometimes expanding events can cause many rows to be created. If the number of new rows exceeds a certain maximum, a popup window asks you to confirm that you want to continue.

To expand a cell, follow these steps:

Step 1 Select a cell in Event Viewer.

The selected cell is highlighted and outlined in gray.

Step 2 To expand a cell by one column, select **Edit > Expand > One Column**.

Step 3 To expand a cell by first group, select **Edit > Expand > First Group**.

Step 4 To expand a cell all the way, select **Edit > Expand > All Columns**.

Saving Your Preferred Column Setting

This procedure explains how to specify and save the following information for a particular event type:

- Which columns are displayed.
- The order in which the columns are displayed.
- The sorting scheme for each column.

Note This procedure is not available in Security Monitor versions 1.1 and earlier.

To save your column setting as your preferred column setting, follow these steps:

Step 1 Start Event Viewer as explained in Starting Event Viewer, page 4-13. In Step 3 of Starting Event Viewer, page 4-13, be sure to select **Last Saved** from the Column Set list box.

Step 2 Drag and drop columns, and delete columns, to arrange them the way you want. Also, sort the columns in ascending or descending order by clicking the column headings.

Step 3 Select **Edit > Save Column Set**.

Your current column setting is saved as your preferred column setting. It applies for the particular event type that you are monitoring when you are the user.

Suspending and Resuming New Events

You can suspend new events from being added to the current Event Viewer display. You can resume receiving new events when you are ready.

To suspend or resume events, follow these steps:

Step 1 To suspend receiving new events, select **Actions > Suspend New Events**.

Event Viewer stops querying the database for new events.

Step 2 To resume receiving new events, select **Actions > Resume New Events**.

Event Viewer resumes querying the database for new events.

Specifying Event Viewer Preferences

Use the options in the Preferences dialog box to specify Event Viewer settings for the current Event Viewer display. To modify preferences for all Event Viewer displays, see Defining Default Event Viewer Preferences, page 4-28 and Defining Custom Event Viewer Preferences, page 4-30.

To specify the Event Viewer preferences, follow these steps:

Step 1 Select **Edit > Preferences**.

The Preferences dialog box appears.

Step 2 To determine how long, in seconds, Event Viewer will wait for a response from the remote sensor or host before concluding that the remote sensor or host is not connected, enter a value in Command Timeout field. The default is 10 seconds.

Step 3 To specify how long, in minutes, a sensor blocks traffic from a specified source when you issue a Block command from Event Viewer, enter a value in the Time to Block field. The default is 1440 minutes.

Step 4 Specify the subnet mask in the Subnet Mask field. This is the mask used to derive the network address from a source address when blocking networks based on a specific event.

Step 5 Configure the grid display behavior. Select the check box that corresponds to the desired behavior:

Select...	To set this behavior...
Blank Left	When multiple, contiguous rows contain the same information in a column, selecting this option causes the first instance of the information to display and subsequent instances to appear blank. When this option is cleared, the repeated information appears in every row. This option is selected by default.
Blank Right	A group of events is typically shown in a single row, with the first column (not counting the Count column) on the left defining the group. Multiple entries in associated columns are shown with a + (plus) sign in the column. Double-clicking the cell with the + sign expands the group by adding rows. When Blank Right is selected, the + sign appears even when there is only one member of a group. You have to expand the group to see the details for the one event. When Blank Right is cleared, a group of events with only one event will show the information for the single event on the top line; you do not need to "drill down" to the single event. Blank Right is cleared by default.

Step 6 Specify whether events are sorted by count or content:

a. To sort events based on the number of events per row from highest to lowest, click the **Count** radio button.

b. To sort events alphabetically based on the column to the right of the Count column, click the **Content** radio button.

Step 7 Specify the default Event Expansion Boundary in the Default Expansion Boundary field.

Step 8 To specify the maximum number of events that can be displayed in a single grid, enter a value in the Maximum Events per Grid field.

Step 9 Specify whether Event Viewer uses colors or icons to indicate event severity.

a. To use colors to display event severity, click the **Color** radio button.

b. To use icons to display event severity, click the **Icon** radio button.

Step 10 To enable automatic queries of the database for new events, select the **Auto Query Enabled** check box.

Step 11 To specify how often, in minutes, Event Viewer queries the database for new events, enter a value in the Query Interval (minutes) field.

Step 12 To save your changes, click **OK**.

Viewing the Context Buffer

A context buffer records exactly what traffic was traversing the network at the time the alarm's signature was detected. Not all signatures contain context buffers. For more information, see Context Buffer, page 4-8.

To view the context buffer, follow these steps:

Step 1 Select a cell in Event Viewer.

The selected cell is highlighted and outlined in gray.

Step 2 Select **View > Context Buffer**.

If the signature has a context buffer, the dialog box displays the context buffer information. Otherwise, the dialog box displays the following message: `No context buffer data for the selected cell.`

Viewing Hostnames

You can view the hostnames that correspond to the source and destination addresses. If a hostname cannot be resolved, you receive a message that the name cannot be resolved.

To view the hostnames, follow these steps:

Step 1 Select a cell in Event Viewer.

The selected cell is highlighted and outlined in gray.

Step 2 Select **View > Hostnames**.

The Hostname Resolution dialog box displays the addresses and corresponding hostnames, if available.

Graphing Event Viewer Data

You can create a graph of the data, or a subset of the data, shown in Event Viewer. The graphs do not update dynamically; they provide a static view of the data at the time the graph was created.

To view a graph of Event Viewer data, follow these steps:

Step 1 Select the events to graph.

- To select all events, select the top-left cell in the display (the root node).
- To select a subset of events, select the cell that corresponds to the events you want to graph.

Step 2 To see how the selected events were distributed over time, select **Graph > By Time** from the menu.

The graph displays along the x-axis the range of time over which the event occurred; along the y-axis the number of occurrences. Event severity is indicated by the color of the bar.

Step 3 To see the distribution of child events, select **Graph > By Child** from the menu.

The graph displays the child events (the events in the column to the right of the selected node) across the X-axis of the graph and the number of occurrences along the Y-axis. Event severity is indicated by the color of the bar.

Step 4 To close the graph, click the close button (designated by the X icon) in the upper-right corner of the graph window.

Learning About Attacks

The Network Security Database (NSDB) provides detailed information about signatures, including descriptions, versions, benign triggers, and related vulnerabilities. You can access the NSDB information for a signature directly from Event Viewer.

To access the NSDB, follow these steps:

Step 1 Select a cell in Event Viewer.

The selected cell is highlighted and outlined in gray.

Step 2 Select **View > Network Security Database**.

If there is an NSDB entry for the event you selected, the NSDB opens in a new window. Otherwise, a dialog box notifies you that there is not an NSDB entry for the event you selected and the NSDB index page opens.

Viewing Event Statistics

You can view event statistics for a cell in Event Viewer. The statistics can include the following:

- The number of events represented by the cell.
- The severity level.
- The number of child cells.
- The percentage of total events that the selected cell and its child cells represent in the current Event Viewer display.

To view event statistics, follow these steps:

Step 1 Select a cell in Event Viewer.

The selected cell is highlighted and outlined in gray.

Step 2 Select **View > Statistics**.

The Event Statistics dialog box displays the event statistics.

Refreshing Events

Based on the settings you specified in the Preferences dialog box, Event Viewer queries the database at regular intervals for new events. If you want to check for new events between intervals or if you have automatic queries disabled, you can use the Refresh Events option to query the database for new events manually.

To refresh the Event Viewer events, follow these steps:

Step 1 Select **Actions > Refresh Events**.

The Event Viewer display is refresh to include any new events.

Step 2 Repeat Step 1 as often as you would like to query for new events.

Blocking a Host or a Network

Blocking a host causes a sensor to block all traffic emanating from the source IP address associated with the selected event. In a similar way, blocking a network causes the sensor to block all traffic emanating from the network that contains the source IP address of the selected event. Blocking is accomplished through a properly configured Cisco router. For information about removing a block, see Removing a Block, page 4-27.

Note The Event Viewer in Security Monitor versions 1.2 and earlier does not support blocking when you are using sensors that are operating with IDS 4.x software.

To block a host or a network, follow these steps:

Step 1 To select an event whose source (a host or a network) you want to block, click the corresponding cell in Event Viewer.

The selected cell is highlighted and outlined in gray.

Step 2 To block a host, select **Block > Host**.

The traffic is blocked for the number of minutes specified in the Preferences dialog box.

Step 3 To block a network, select **Block > Net**.

The traffic is blocked for the number of minutes specified in the Preferences dialog box.

Note The network address of a blocked network is calculated by applying the network mask in the Preferences panel to the source IP address of the selected event.

Removing a Block

You can remove any blocks that you have added in Event Viewer.

Note Security Monitor versions 1.2 and earlier do not support blocking when you are using sensors that are operating with IDS 4.x software.

To remove a block, follow these steps:

Step 1 To select the event from which you want to remove the block, select the corresponding cell in Event Viewer.

The selected cell is highlighted and outlined in gray.

Step 2 To remove a sensor's block from a host, select **Remove Block > Host**.

Step 3 To remove a sensor's block from a network, select **Remove Block > Net**.

Step 4 To remove all blocks, select **Remove Block > All**.

Defining Event Viewer Preferences

This section describes how to define Event Viewer preferences. It also describes how to administer preferences of Event Viewer users. This section contains the following procedures:

- Defining Default Event Viewer Preferences, page 4-28
- Defining Custom Event Viewer Preferences, page 4-30
- Viewing Event Viewer Users, page 4-32
- Deleting Users from the Event Viewer Database, page 4-32

Defining Default Event Viewer Preferences

If you have administrative privileges, you can define the default Event Viewer preferences. Default preferences are used by all users. However, users can define custom preferences to reconfigure their views. For more information, see Defining Custom Event Viewer Preferences, page 4-30.

To define the default Event Viewer preferences, follow these steps:

Step 1 Select **Admin > Event Viewer**.

Step 2 Select **Default Preferences** from the TOC.

The Default Preferences page appears.

Step 3 To determine how long, in seconds, Event Viewer will wait for a response from the remote sensor or host before concluding that the remote sensor or host is not connected, enter a value in Command Timeout field. The default is 10 seconds.

Step 4 To specify how long, in minutes, a sensor blocks traffic from a specified source when you issue a Block command from Event Viewer, enter a value in the Time to Block field. The default is 1440 minutes.

Step 5 Specify the subnet mask in the Subnet Mask field.

Step 6 Specify the default Event Expansion Boundary in the Default Expansion Boundary field.

Step 7 Enter a value in the Maximum Events per Grid field to specify the maximum number of events that can be displayed in a single grid.

Step 8 To specify how often, in minutes, Event Viewer queries the database for new events, enter a value in the Query Interval (minutes) field.

Step 9 To enable automatic queries of the database for new events, select the **Auto Query Enabled** check box.

Step 10 Specify whether Event Viewer uses colors or icons to indicate event severity.

a. To use colors to display event severity, click the **Color** radio button.

b. To use icons to display event severity, click the **Icon** radio button.

Step 11 Configure the grid display behavior. Select the check box that corresponds to the desired behavior:

Select...	To set this behavior...
Blank Left	When multiple, contiguous rows contain the same information in a column, selecting this option causes the first instance of the information to display and subsequent instances to appear blank. When this option is cleared, the repeated information appears in every row. This option is selected by default.
Blank Right	A group of events is typically shown in a single row, with the first column (not counting the Count column) on the left defining the group. Multiple entries in associated columns are shown with a + (plus) sign in the column. Double-clicking the cell with the + sign expands the group by adding rows. When Blank Right is selected, the + sign appears even when there is only one member of a group. You have to expand the group to see the details for the one event. When Blank Right is cleared, a group of events with only one event will show the information for the single event on the top line; you do not need to "drill down" to the single event. Blank Right is cleared by default.

Step 12 Specify whether events are sorted by count or content.

a. To sort events based on the number of events per row from highest to lowest, click the **Count** radio button.

b. To sort events alphabetically based on the column to the right of the Count column, click the **Content** radio button.

Step 13 Click **Apply**.

The preferences you specified are the default preferences used by all Event Viewer users.

Defining Custom Event Viewer Preferences

You can define custom Event Viewer preferences that override the default Event Viewer preferences. Custom Event Viewer preferences affect only the Event Viewer displays opened by the user for whom the preferences were defined.

To define custom Event Viewer preferences, follow these steps:

Step 1 Select **Admin > Event Viewer**.

Step 2 Select **Your Preferences** from the TOC.

The Your Preferences page appears.

Step 3 To determine how long, in seconds, Event Viewer will wait for a response from the remote sensor or host before concluding that the remote sensor or host is not connected, enter a value in Command Timeout field. The default is 10 seconds.

Step 4 To specify how long, in minutes, that a sensor blocks traffic from a specified source when you issue a Block command from Event Viewer, enter a value in the Time to Block field. The default is 1440 minutes.

Step 5 Specify the subnet mask in the Subnet Mask field.

Step 6 Specify the default Event Expansion Boundary in the Default Expansion Boundary field.

Step 7 Enter a value in the Maximum Events per Grid field to specify the maximum number of events that can be displayed in a single grid.

Step 8 To specify how often, in minutes, that Event Viewer queries the database for new events, enter a value in the Query Interval (minutes) field.

Step 9 To enable automatic queries of the database for new events, select the Auto Query Enabled check box.

Step 10 Specify whether Event Viewer uses colors or icons to indicate event severity.

a. To use colors to display event severity, click the Color radio button.

b. To use icons to display event severity, click the Icon radio button.

Step 11 Configure the grid display behavior. Select the check box that corresponds to the desired behavior:

Select...	To set this behavior...
Blank Left	When multiple, contiguous rows contain the same information in a column, selecting this option causes the first instance of the information to display and subsequent instances to appear blank. When this option is cleared, the repeated information appears in every row. This option is selected by default.
Blank Right	A group of events is typically shown in a single row, with the first column (not counting the Count column) on the left defining the group. Multiple entries in associated columns are shown with a + (plus) sign in the column. Double-clicking the cell with the + sign expands the group by adding rows. When Blank Right is selected, the + sign appears even when there is only one member of a group. You have to expand the group to see the details for the one event. When Blank Right is cleared, a group of events with only one event will show the information for the single event on the top line; you do not need to "drill down" to the single event. Blank Right is cleared by default.

Step 12 Specify whether events are sorted by count or content.

a. To sort events based on the number of events per row from highest to lowest, click the **Count** radio button.

b. To sort events alphabetically based on the column to the right of the Count column, click the **Content** radio button.

Step 13 To save your changes, click **Apply**.

Your Event Viewer displays will use the preferences you defined.

Step 14 To revert to the default Event Viewer preferences, click **Reset to Defaults**.

Your custom preferences are overwritten by the default preferences used by all Event Viewer users.

Viewing Event Viewer Users

You can view a list of users that have custom Event Viewer preferences stored in the database.

To view a list of Event Viewer users, follow these steps:

Step 1 Select **Admin > Event Viewer**.

Step 2 Select **Users** from the TOC.

The Users page appears. The users are listed in a table on this page.

Deleting Users from the Event Viewer Database

To clean up your database, you can delete preferences for users who no longer view events. Only the event viewing preferences for that user are deleted from the database.

Note You must have administrative privileges to delete user preferences from the database.

Tip Security Monitor administers only Event Viewer user records. To administer user permissions, you must use IDS MC. For more information, refer to *Using Management Center for IDS Sensors*.

To delete a user from the Event Viewer database, follow these steps:

Step 1 Select **Admin > Event Viewer**.

Step 2 Select **Users** from the TOC.

The Users page appears.

Step 3 To select which user to delete, select the check box next to the user ID.

Note You can select all users by clicking Select All.

A check mark appears next to the user ID that you selected.

Step 4 To delete Event Viewer preferences for the selected user, click **Delete**.

The event viewing preferences for the selected user are deleted from the Event Viewer database.

Cisco Intrusion Detection System Sensor Configuration Note Version 3.1

May 2002

This publication describes the version 3.1 sensor and includes configuration and upgrade procedures.

Contents

Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Upgrading an Existing Sensor

The following section describes how to upgrade an existing sensor from version 3.0 to 3.1, how to re-image a 3.1 sensor, and how to uninstall version 3.1.

This section includes these topics:

- Downloading from Cisco.com
- Using the CD
- Uninstalling Version 3.1

Downloading from Cisco.com

You can upgrade from version 3.0 to 3.1 by downloading the new version from Cisco.com.

To download the 3.1 upgrade, follow these steps:

Step 1 Download the self-extracting binary file from Cisco.com found at the following website:

http://www.cisco.com/cgi-bin/tablebuild.pl/ids-appsens

Step 2 Copy the binary file IDSk9-sp-3.1-1-S22.bin to the /tmp directory on the target sensor.

Caution You must use the original filename.

Step 3 Log in as root on the sensor.

Step 4 Change the attributes of the binary file to an executable file by typing the following:

```
chmod +x IDSk9-sp-3.1-1-S22.bin
```

Step 5 Start the binary file installation with the `-I` option by typing the following:

```
IDSk9-sp-3.1-1-S22.bin -I
```

Step 6 Review the file output.log in /usr/nr/sp-update for the status of this Service Pack after the installation is complete.

Using the CD

With the sensor upgrade/recovery CD you can upgrade a sensor to version 3.1 or restore a version 3.1 sensor to the initial factory version 3.1 software installation.

This section includes these topics:

- Upgrading with the CD, page 27
- Re-Imaging with the CD, page 27

Upgrading with the CD

If you are running version 2.5(x), you must upgrade to version 3.0(1)S4. You can upgrade version 2.5 sensors to version 3.0 using the following self-extracting binary file:

IDSk9-sp-3.0-1-S4.bin

This binary file is available at the following website:

http://www.cisco.com/cgi-bin/tablebuild.pl/ids-appsens

Note You must have a SMARTnet maintenance contract number to request software upgrades from Cisco.com.

To upgrade the sensor from version 3.0 to 3.1, follow these steps:

Step 1 Insert the CD.

Step 2 Log in as root.

Step 3 Type the following at the prompt:

```
mount_cd
```

The installation begins.

Re-Imaging with the CD

Caution The sensor upgrade/recovery CD erases all contents of the hard-disk drive of the sensor. All configuration data stored on the sensor is overwritten.

This section includes these topics:

Using the IDS Device Manager

To re-image a 3.1 sensor, follow these steps:

Step 1 Open a web browser and type the web address of the IDS Device Manager:

`https://`*sensor ip address*

Step 2 Type the username at the prompt:

`netrangr` (default)

Step 3 Type the password at the prompt.

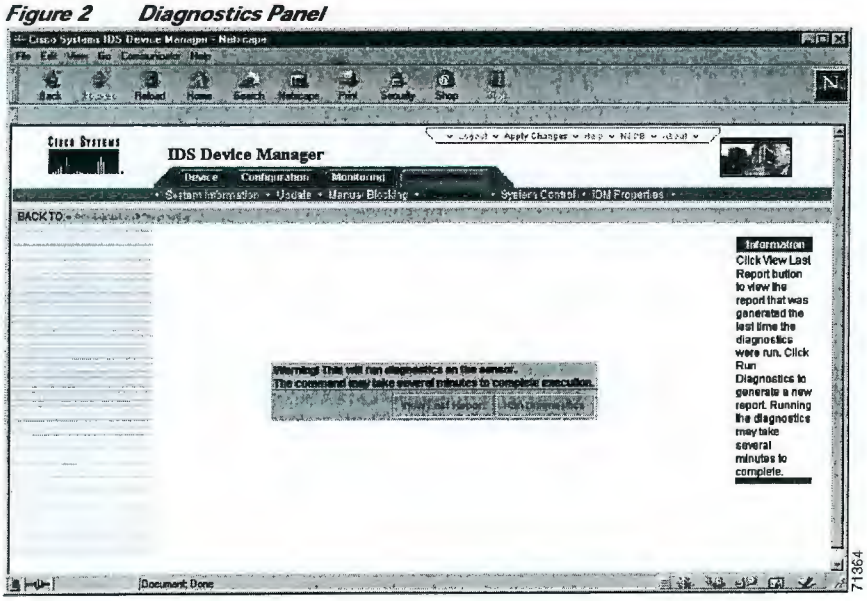
Result: The IDS Device Manager appears.

Figure 1 IDS Device Manager

Step 4 Select **Administration > Diagnostics**.

Result: The Diagnostics panel appears.

Figure 2 Diagnostics Panel



Step 5 Click **Run Diagnostics**.

Step 6 When the diagnostics are complete, click **View Diagnostics**.

Result: The diagnostics report appears in another browser window.

Step 7 Select **File > Save As** in your browser to save the page for use with Step 21 when you are reconfiguring sysconfig-sensor.

Step 8 Insert the upgrade/recovery CD into the CD-ROM drive.

Step 9 Connect with a terminal, or attach a monitor and keyboard to the sensor.

Step 10 Log in as root.

Step 11 Enter the username `root` and the default password `attack` at the prompt.

Step 12 Reboot the sensor by typing:

```
init 6
```

Step 13 As the sensor reboots, press **F2** to enter the Setup Menu.

Step 14 Verify that the boot sequence is Floppy Drive, CD-ROM, and Hard Drive.

This boot sequence is required so that the system boots to the Recovery/Upgrade CD when it is restarted.

Note You only need to perform Step 14 once on each system unless the BIOS settings become modified or corrupted.

Step 15 Exit the Setup menu, saving changes to the boot sequence if necessary.

Step 16 After the sensor boots, you are prompted to install from the console (option `c`) or from a remote/serial terminal connection (option `t`).

Note The CD defaults to option `t` after 10 seconds allowing for remote connections. Keyboard input at this stage of the installation is not supported.

Step 17 After re-imaging the sensor, log in as root.

Step 18 Enter the username `root` and the default password `attack` at the prompt.

Step 19 Type `sysconfig-sensor` at the prompt.

Step 20 Configure options 1through 6 with the information that you saved in Step 7.

Step 21 Save your changes and exit the sysconfig-sensor utility.

Step 22 The sensor reboots.

Note The password is reset to "attack" (default). To maintain security, change the default password for netrangr immediately by selecting **Device > Sensor Setup > Password** in the IDS Device Manager.

Using sysconfig-sensor

To use sysconfig-sensor and the CD to re-image a sensor, follow these steps:

Step 1 Connect with a terminal, or attach a monitor and keyboard to the sensor.

Step 2 Log on as user root.

Step 3 Type `sysconfig-sensor` at the prompt.

Step 4 Record the values for the following fields:

- IP Address
- IP Netmask
- IP Host Name
- Default Route
- Network Access Control
- Allowed Host
- Communications Infrastructure
- Sensor Host ID
- Sensor Organization ID
- Sensor Host Name
- Sensor Organization Name
- IDS Manager Host ID
- IDS Manager Organization ID
- IDS Manager Host Name
- IDS Manager Organization Name
- IDS Manager IP Address

Step 5 If secure communications is enabled, record the values on the following fields on the Session Keys screen:

- Current Inbound Configuration [IDS Manager to Sensor]
- Cipher Key
- Authentication Key
- SPI
- Current Outbound Configuration [Sensor to IDS Manager]
- Cipher Key
- Authentication Key
- SPI

Step 6 Insert the upgrade/recovery CD into the CD-ROM drive.

Step 7 Connect with a terminal, or attach a monitor and keyboard to the sensor.

Step 8 Enter the username `root` and the default password `attack` at the prompt.

Step 9 Reboot the sensor by typing:

```
init 6
```

Step 10 As the sensor reboots, press **F2** to enter the Setup Menu.

Step 11 Verify that the boot sequence is Floppy Drive, CD-ROM, and Hard Drive.

This boot sequence is required so that the system boots to the recovery/upgrade CD when it is restarted.

Note You only need to perform Step 11 once on each system unless the BIOS settings become modified or corrupted.

Step 12 Exit the Setup menu, saving changes to the boot sequence if necessary.

Step 13 After the sensor boots, you are prompted to install from the console (option `c`) or from a remote/serial terminal connection (option `t`).

Note The CD defaults to option `t` after 10 seconds for remote connections. Keyboard input at this stage of the installation is not supported.

Step 14 After re-imaging the sensor, enter the username `root` and the default password `attack` at the prompt.

Step 15 Type `sysconfig-sensor` at the prompt.

Step 16 Configure options 1 through 6 with the information that you saved in Steps 4 and 5.

Step 17 Save your changes and exit the sysconfig-sensor utility.

The sensor reboots.

Note The password is reset to "attack" (default). To maintain proper security, change the default password for netrangr immediately by configuring option 8 in sysconfig-sensor, or by logging in as user netrangr after the sensor reboots and changing the password at the prompt.

Uninstalling Version 3.1

To uninstall the sensor 3.1 upgrade, follow these steps:

Step 1 Log in as root.

Step 2 Execute the binary file with the `-U` option by typing the following:

```
IDSk9-sp-3.1-1-S22.bin -U
```

Upgrading Signatures

Signatures are upgraded every two weeks and the upgrade is posted on Cisco.com.

This section includes these topics:

Downloading from Cisco.com

You can download signature upgrades with instructions for installing them at the following website:

http://www.cisco.com/kobayashi/sw-center/

You must have access to the website.

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 download signature update and service packs from Cisco.com. You must download the signature update or service pack to your own FTP server, and then configure the sensor to download them from your FTP server.

Automatic Updates

You can schedule the sensor to download signature and service pack updates from a designated FTP server and apply them.

Note If you are using the IDS Device Manager as your IDS manager, select **Administration > Update** to configure automatic updates. For more information, refer to the *Cisco Intrusion Detection System Device Manager Configuration Note version 3.1* found at the following website:
http://www.cisco.com/univercd/cc/td/doc/product/iaabu/csids/csids8/index.htm

To have the sensor download and apply updates, follow these steps:

Step 1 Choose a remote computer on which to store the sensor updates.

Step 2 Make sure the computer is running an FTP server.

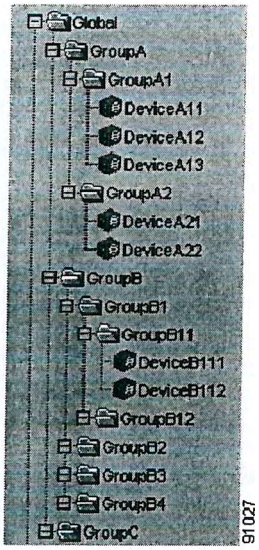
The sensor uses an FTP client to download the updates.

Note The FTP server does not have to be a sensor, but we do recommend a sensor, because the OS has already been secured. See the "Supported FTP Servers" section on page 32 for a list of supported FTP servers.

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.

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.

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.

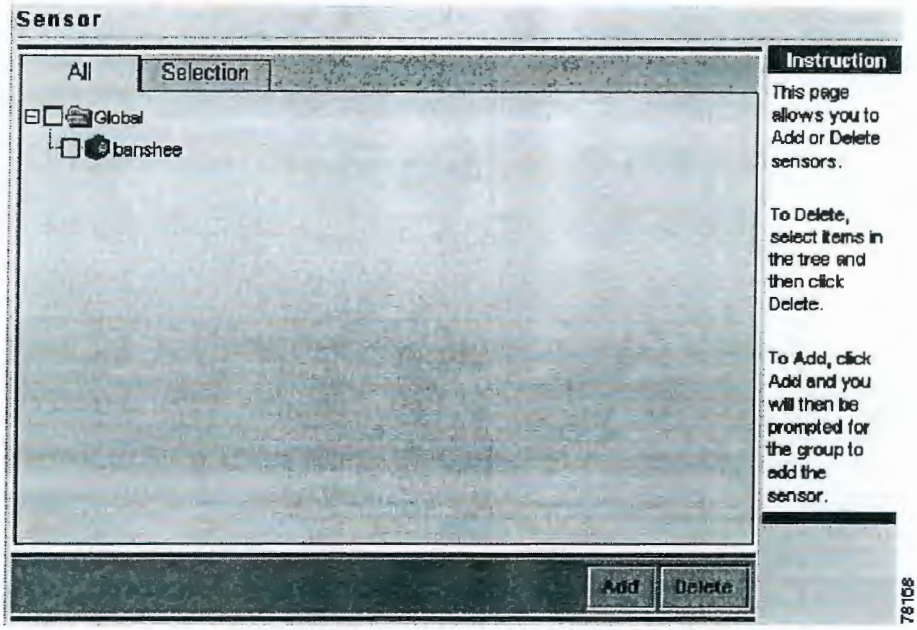
Adding Sensors to a Sensor Group

You can add a sensor to any sensor group, including the Global group.

To add a sensor to a sensor group, follow these steps:

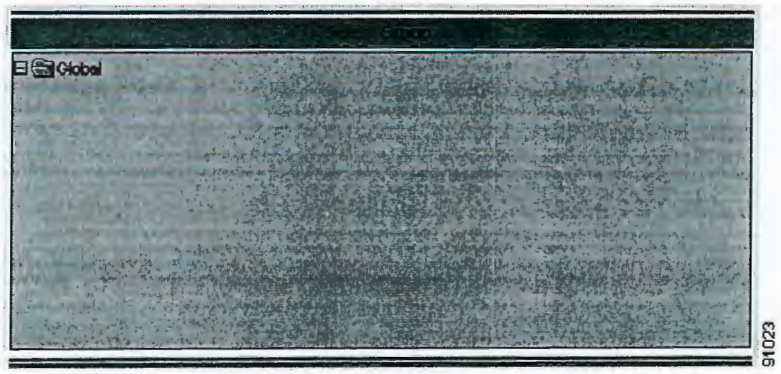
Step 1 Select **Devices > Sensor**.

The Sensor page appears.



Step 2 Click **Add**.

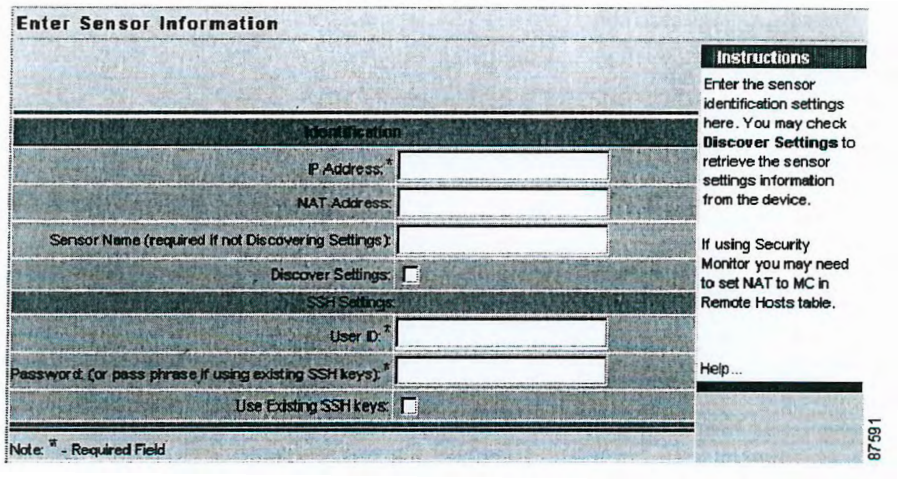
The Select Group page appears.



Step 3 Select the group you want to add a sensor to.

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.

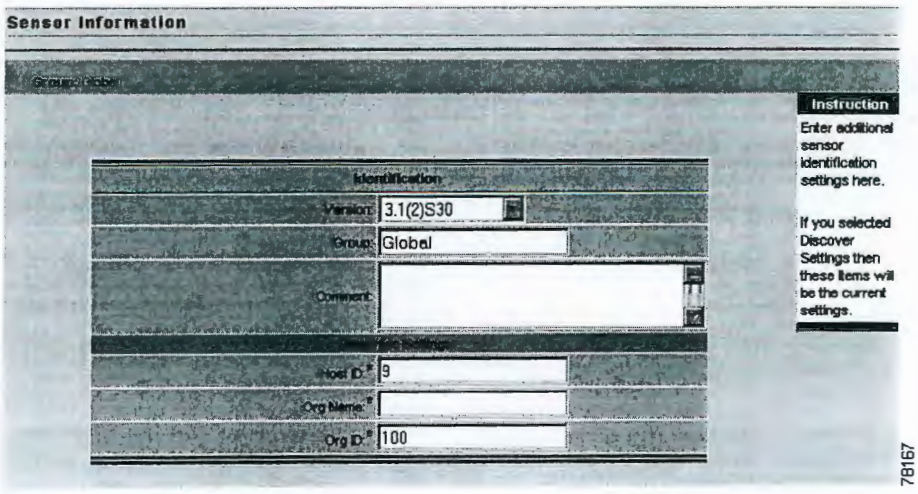
f. If you want to use existing SSH keys, select the check box associated with that option. However, you cannot use SSH keys if you intend to use this sensor as a master blocking sensor.

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.



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.

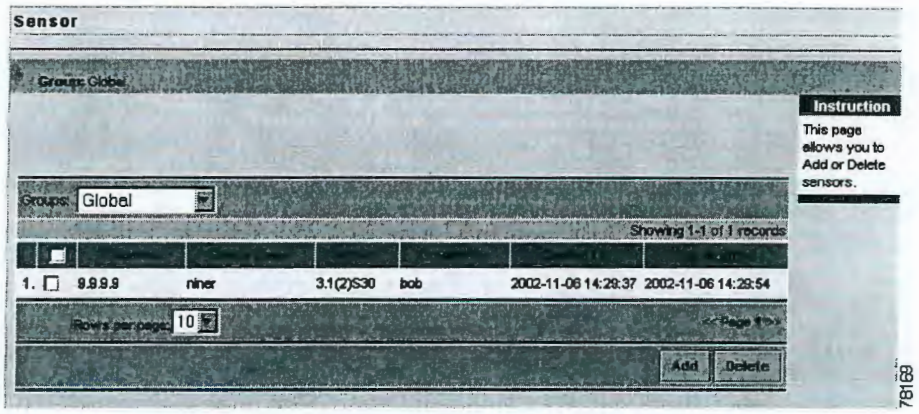
Step 7 If you are using IDS MC 1.1 *and* you are adding a sensor operating with sensor software 4.x, provide the following information in the Sensor Information page:

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.



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

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.

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.
```

"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.

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.

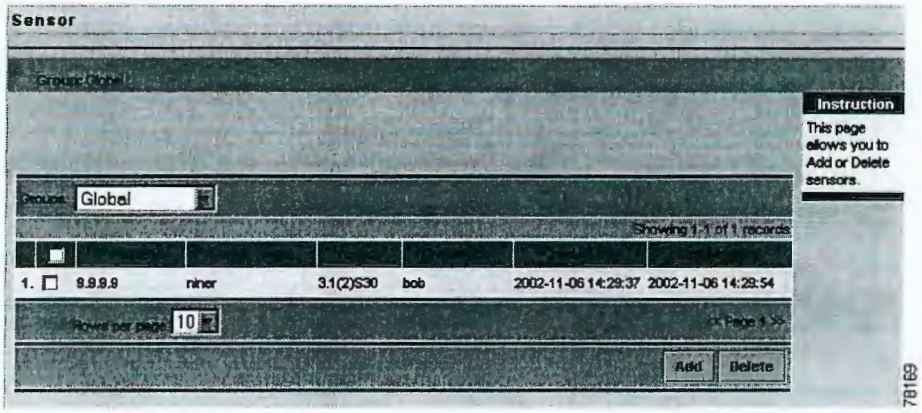
Deleting Sensors from a Sensor Group

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.

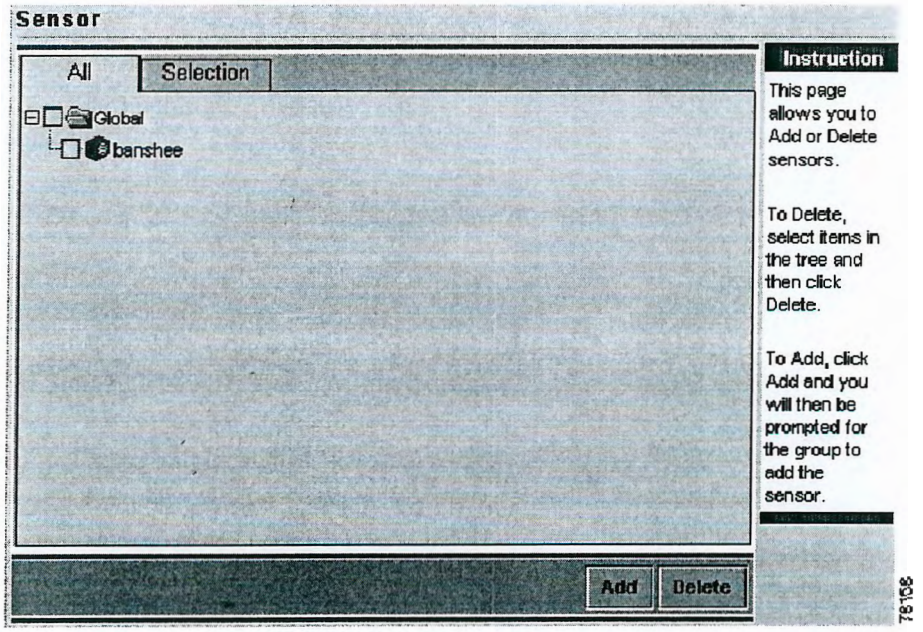


Step 2 In the tree, select the sensor that you want to delete.

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.



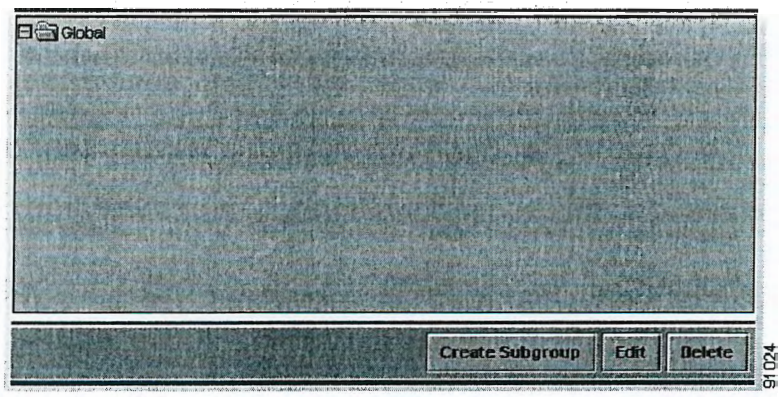
Creating Sensor Subgroups

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**.

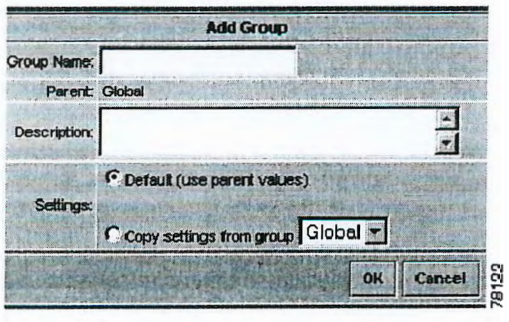
The Sensor Group page appears.



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**.

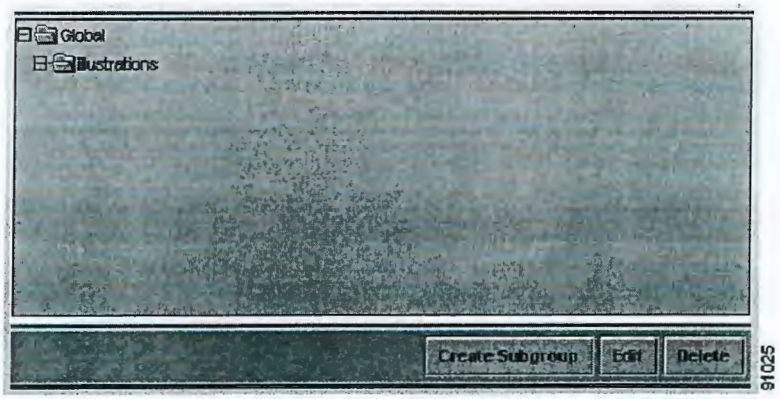
The Add Group page appears.



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.



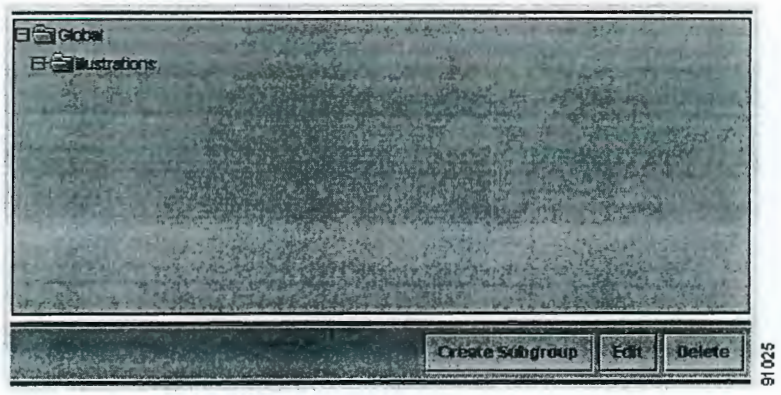
Deleting Sensor Groups

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.



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.

SunOS NIS Vulnerabilities

General Affected External

General

Relat
TAC (
TAC (
TAC (
Dynai

Key Attributes

Attributes/Severity	**Low Severity**
Vulnerability Type:	Network
Exploit Type:	Access

Description
NIS systems contain password maps, which an attacker can obtain and then use for cracking passwords. To obtain copies of maps, an attacker only needs to know the domain name, which is often set to the DNS domain name by administrators. Also, an attacker can get the domain name by guessing the name of a diskless client that boots from a server running rpc.bootparamd.

Consequences
An attacker can obtain copies of NIS password maps.

Countermeasures
Run NIS+ instead of NIS. You can also use an obscure name as the NIS domain name, though this is not a complete fix, since there are other ways of obtaining the domain name.

Products
Scanner xxx
CSS Versions: 2.0
IDS Signature ypserv Portmap Request
SignatureId/ SubId 6150/0
CSID Versions: 2.1.1
Signature Description Triggers when a request is made to the portmapper for the YP server daemon (ypserv) port. The ypserv daemon is responsible for looking up information maintained in NIS maps. This may be indicative of an attempt to gain unauthorized access to system resources.
Alarm Level 2
Benign Triggers If this procedure is allowed on your network, those users that employ it will trigger the signature.
Signature Type NETWORK
Signature Structure ATOMIC
Implementation CONTENT
IDS Signature ypbind Portmap Request
SignatureId/ SubId 6151/0
CSID Versions: 2.1.1
Signature Description Triggers when a request is made to the portmapper for the YP bind daemon (ypbind) port. The ypbind daemon is responsible for maintaining the information needed for a client process to communicate with a ypserv process. This may be indicative of an attempt to gain unauthorized access to system resources.

Alarm Level 2
Benign Triggers If this procedure is allowed on your network, those users that employ it will trigger the signature.
Signature Type NETWORK
Signature Structure ATOMIC
Implementation CONTENT

IDS Signature yppasswdd Portmap Request
SignatureId/ SubId 6152/0
CSID Versions: 2.1.1
Signature Description Triggers when a request is made to the portmapper for the YP password daemon (yppasswdd) port. The YP password daemon allows users to remotely modify password files. This may be indicative of an attempt to gain unauthorized access to system resources.
Alarm Level 2
Benign Triggers If this procedure is allowed on your network those users that employ it will trigger the signature. This may be a serious attempt at gaining unauthorized access and if the source of the attempt is not within your network they should be shunned.
Signature Type NETWORK
Signature Structure ATOMIC
Implementation CONTENT

IDS Signature ypxfrd Portmap Request
SignatureId/ SubId 6154/0
CSID Versions: 2.1.1
Signature Description Triggers when a request is made to the portmapper for the YP transfer daemon (ypxfrd) port. The YP transfer daemon is responsible for transferring NIS information on behalf of ypserv. This may be indicative of an attempt to gain unauthorized access to system resources.
Alarm Level 2
Benign Triggers If this procedure is allowed on your network, those users that employ it will trigger the signature.
Signature Type NETWORK
Signature Structure ATOMIC
Implementation CONTENT

Affected

Affected Operating Systems

Operating System	Versions
SunOS [PATCH]	3.x,4.x

Affected Software and Programs

Software	Versions	Program Versions
NIS [PATCH]	Any	

Affected Services

Name	Type	Ports	RPC
RPC	File_sharing	111/TCP 111/UDP	rwall/100008 cmsd/100068 ttdbserverd/100083 sprayd/100012 rstatd/100001 amd/300019 ypbind/100007 yppasswd/100009 mountd/100005 pcnfsd/150001 amd/100065 portmapper/100000 rquotad/100011 selection_svc/100015 rexd/100017 YPServ/100004 ypupdated/100028

sadmind/100232
bootparam/100026

External Advisories

Advisory Name	Advisory Source
CA-92:13.SunOS.NIS.vulnerability>>Read	BUGTRAQ

Links

General Information
NONE

HP ypbind

General Affected External

General

Relat
TAC (
TAC (
TAC (
Dynai

Key Attributes

Attributes/Severity	**Low Severity**
Vulnerability Type:	Network
Exploit Type:	Access

Description
NIS on HP systems allows unauthorized access to NIS data.

Consequences
An attacker who gains root access on a remote host running any vendor's implementation of NIS can also gain root access on any local host running HP's NIS ypbind. A local user of a host running HP's NIS ypbind can also gain root access.

Countermeasures
All HP NIS clients and servers running ypbind should obtain and install the patch appropriate for their machine's architecture. For additional information, please see the CERT advisory: ftp://info.cert.org/pub/cert_advisories/CA-93:01.REVISED.HP.NIS.ypbind.vulnerability

Products
Scanner xxx
CSS Versions: 2.0
IDS Signature ypbind Portmap Request

SignatureId/ SubId	6151/0
CSID Versions:	2.1.1
Signature Description	Triggers when a request is made to the portmapper for the YP bind daemon (ypbind) port. The ypbind daemon is responsible for maintaining the information needed for a client process to communicate with a ypserv process. This may be indicative of an attempt to gain unauthorized access to system resources.
Alarm Level	2
Benign Triggers	If this procedure is allowed on your network, those users that employ it will trigger the signature.
Signature Type	NETWORK
Signature Structure	ATOMIC
Implementation	CONTENT

Affected
Affected Operating Systems

Operating System	Versions
HP-UX [PATCH]	8.x

Affected Software and Programs

Software	Versions	Program Versions
NIS		

[PATCH]Any

Affected Services

Name Type	Ports	RPC
RPC File_sharing	111/TCP 111/UDP	rwall/100008 cmsd/100068 ttdbserverd/100083 sprayd/100012 rstatd/100001 amd/300019 ypbind/100007 yppasswd/100009 mountd/100005 pcnfsd/150001 amd/100065 portmapper/100000 rquotad/100011 selection_svc/100015 rexd/100017 YPServ/100004 ypupdated/100028 sadmind/100232 bootparam/100026

External
CVE Information
CVE ID: CVE-1999-0312

Advisories

Advisory Name	Advisory Source
CA-93:01.REVISED.HP.NIS.ypbind.vulnerability>>Read	CERT

Links
General Information
Advisory Source

TECHNICAL SUPPORT

Cisco Secure Encyclopedia

RPC Port Unregistration

General Affected External

General

Key Attributes

Attributes/Severity	**Medium Severity**
Vulnerability Type:	Network
Exploit Type:	Denial

Description
The portmapper allows port registration and unregistration requests from other machines. These requests should come only from the host.

Consequences
An attacker could unregister services and cause a denial of service.

Countermeasures
Filter out portmapper registration and unregistration requests at the router or firewall. Upgrade to Wietse's secure version of RPCBIND 2.1 or later (URL listed in the Links). Cisco Systems' NetRanger will detect these type of attacks.

Products
Scanner xxx
CSS Versions: 2.0
IDS Signature RPC Port Registration

SignatureId/ SubId	6100/0
CSID Versions:	1.0
Signature Description	Triggers when attempts are made to register new RPC services on a target host. Port registration is the method used by new services to report to the portmapper that they are present and to gain access to a port, this is then advertised by the portmapper. This should not be allowed from a remote host. No known exploit of this function exists. This does not preclude the possibility that exploits do exist outside of the realm of Cisco Systems knowledge domain.
Alarm Level	5
Benign Triggers	No known triggers.
Signature Type	NETWORK
Signature Structure	ATOMIC
Implementation	CONTENT

IDS Signature RPC Port Unregistration

SignatureId/ SubId	6101/0
CSID Versions:	1.0
Signature Description	Triggers when attempts are made to unregister existing RPC services on a target host. Port unregistration is the method used by services to report to the portmapper that they are no longer present and to remove them from the active port map. This should not be allowed from a remote host. No known

exploit of this function exists. This does not preclude the possibility that exploits do exist outside of the realm of Cisco Systems knowledge domain.

Alarm Level	5
Benign Triggers	No known triggers.
Signature Type	NETWORK
Signature Structure	ATOMIC
Implementation	CONTENT

Affected

Affected Operating Systems

Operating System	Versions
IRIX [PATCH]	6.5
SunOS [PATCH] on SPARC [PATCH]	4.0.3-
Linux [PATCH]on Intel [PATCH]	Any

Affected Software and Programs

Software	Versions	Program	Versions
		rpcbind	Any

Affected Services

Name	Type	Ports	RPC
RPC	File_sharing	111/TCP 111/UDP	rwall/100008 cmsd/100068 ttdbserverd/100083 sprayd/100012 rstatd/100001 amd/300019 ypbind/100007 yppasswd/100009 mountd/100005 pcnfsd/150001 amd/100065 portmapper/100000 rquotad/100011 selection_svc/100015 rexd/100017 YPServ/100004 ypupdated/100028 sadmind/100232 bootparam/100026

External Links

General Information
Fix
General Information

TECHNICAL SUPPORT

Cisco Secure Encyclopedia

DNS Inverse Query Buffer Overflow

General Affected External

General

Key Attributes

Attributes/Severity	**High Severity**
Vulnerability Type:	Network
Exploit Type:	Access

Description
Berkeley Internet Name Domain (BIND) is an implementation of the Domain Name Service (DNS) protocol. It includes a name server called 'named.' Vulnerable versions of the named server fail to properly check incoming inverse query (IQUERY) requests and are subject to buffer overflow attacks.

Consequences
A remote attacker could crash the DNS service or execute arbitrary commands as the user running named. Since inverse queries are disabled by default, an administrator would have had to enable the feature for a system to be vulnerable.

Countermeasures
BIND 8–disable inverse queries, upgrade to BIND 8.1.2, or apply the patch from ftp://ftp.cert.org/pub/cert_advisories/Patches/CA-98.05_Topic.1_BIND8_patch.txt

BIND 4.9–disable inverse queries, upgrade to BIND 4.9.7 (http://www.isc.org/products/BIND/) or apply the patch from ftp://ftp.cert.org/pub/cert_advisories/Patches/CA-98.05_Topic.1_BIND4.9_patch.txt

Access

Access Required:	None
Access Gained:	None

Discovery Date
31-MAY-1998

Products
IDS Signature DNS Inverse Query Buffer Overflow

SignatureId/ SubId	6055/0
CSID Versions:	2.2.1.1
Signature Description	This alarm triggers when an IQUERY request arrives with a data section that is larger than 255 characters.
Alarm Level	5
Benign Triggers	No known triggers.
Signature Type	NETWORK

Signature Structure	ATOMIC
Implementation	CONTENT

Scanner xxx
CSS Versions: 2.0

Affected
Affected Operating Systems

Operating System	Versions
Solaris [PATCH]	2.5.1,2.6,2.5,2.3,2.4
AIX [PATCH]	4.1.x,4.3.x,4.2.x
Redhat Linux [PATCH]	4.2,5.0
HP-UX [PATCH]	Any
IRIX [PATCH]	Any
SCO UnixWare [PATCH]	3.2v4,7,2.1
SCO OpenServer [PATCH]	5.0,3.0
NetBSD [PATCH]	1.3,1.3.1
SCO OpenDesktop [PATCH]	3.0
SCO Internet FastStart [PATCH]	Any

Affected Software and Programs

Software	Versions	Program	Versions
BIND [PATCH]	4.9.5,8.1	BIND	4.9.5

Affected Services

Name	Type	Ports	RPC
DNS	Info_status	53/TCP 53/UDP	

External
CVE Information
CVE ID: CVE-1999-0009

Advisories

Advisory Name	Advisory Source
Bind Problems>>Read	CERT
Security Bulletin #00180>>Read	Sun Microsystems
HPSBUX9808-083: Security Vulnerability in BIND on HP-UX>>Read	SecurityFocus

Links
General Information
Fix

Aliases

Vendor	Product	Alias
Security Focus	Vulnerabilities Database	Multiple Vendor BIND iquery buffer overflow Vulnerability

-

ESL9595L2

A tape library ESL9595L2 possui características que permitem uma alta disponibilidade do ambiente.

Os drives podem ser substituídos online sem parada do servidor ou da aplicação. O dado é automaticamente redirecionado através de outros drives sem necessidade de reconfiguração.

Para manter alta disponibilidade, várias ferramentas de diagnóstico podem prover um rápido isolamento e recuperação de problemas de hardware, incluindo testes no power-on do equipamento.

A limpeza automática do drive aumenta a disponibilidade e elimina a necessidade de manutenção preventiva e seu downtime associado.

A tape library possui componentes redundantes como fontes, ventiladores e PDUs.

Para manter a disponibilidade do ambiente e operação contínua, os drives são hot-

pluggable e as fontes e ventiladores hot-swappable.

Outras informações sobre disponibilidade da tape library ESL9595L2 podem ser obtidas nos catálogos que foram anexados na proposta.

Descrição das Tapes Library

BRASILIA

2 (duas) Hp StorageWorks ESL9595 com:
400 Slots,
20 drives ultrium 460,
5 bridges modelo e2400-160 FC com 20 canais SCSI
1 (um) Pass-through para conecção das ESL9595

SAN Switch

4 (quatro) HP StorageWorks Core Switch 2/64 postas

São Paulo

1 (uma) Hp storageworks ESL9595 com:
400 Slots,
12 drives Ultrium 460,
3 bridges modelo e2400-160 FC com 12 canais SCSI

SAN Switch

2 (dois) HP StorageWorks Core Switch 2/64 portas

Atributo 1 – DESCRIÇÃO

- Estão sendo fornecidos 2 (dois) sistemas automatizados de armazenamento de dados em cartuchos padrão 'LTO Ultrium 2', incorporando controladora robotizada, gabinete e software de gerenciamento. Sendo 1 (um) sistema para o CCD de Brasília-DF e 1(um) sistema para o CCD de São Paulo-SP.

- 02 libraries modelo ESL9595L2 20 drives Brasília (única library lógica) e 01 library ESL9595L2 12 drives São Paulo.

Atributo 2 – Capacidade da Biblioteca

- Para o CCD de Brasília, o equipamento possui capacidade de armazenamento e recuperação de dados para a tecnologia 'LTO Ultrium 2' de 80TB (oitenta Terabytes), sem compressão (nativo);
- Para o CCD de São Paulo, o equipamento possui capacidade de armazenamento e recuperação de dados para a tecnologia 'LTO Ultrium 2' de 80TB (oitenta Terabytes), sem compressão (nativo);

- Não está sendo considerada para efeito de cálculo da capacidade solicitada tecnologia de compactação e/ou compressão.

- Equipamento ofertado: Tape Library ESL9595L2 com 400 slots de fita para Brasília e São Paulo.

Atributo 4 – Compatibilidade -??????

Atributo 5 – Quantidade de SLOTS

Possui um mínimo de SLOTS que disponibiliza a capacidade total solicitada de cada fitoteca dividida pela capacidade dos cartuchos cotados, ou seja:
Num. Slots = Capacidade Solicitada da Biblioteca / Capacidade do Cartucho.

1.Quantidade de slots Brasília = 60TB / 200 Gb = 300 slots

2.Quantidade de slots São Paulo = 40TB / 200 Gb = 200 slots

Atributo 5 – Quantidade de cartuchos

Está sendo ofertado 600 cartuchos para Brasília e 400 cartuchos para São Paulo (= dobro do número de slots solicitados).

- Os cartuchos são testados e garantidos contra erros por um período mínimo de 30 (Trinta) anos, sem manutenção.

Atributo 8 -Numero de Drives

- ESL9595L2 com 12 drives para São Paulo, atingindo throughput de 600 MB/sec sem compressão e ESL9595L2 com 20 drives para Brasília, utilizando mecanismo de pass-through, atingindo throughput de 360 MB/sec sem compressão

Atributo 14 - Fonte de alimentação interna

- O n° de fontes instaladas é suficiente para suportar a operação do equipamento na configuração máxima especificada;

- Possui recurso de troca sem interrupção (HOT-SWAPPABLE);

- Possui alimentação elétrica de acordo com a localidade onde serão instalados os equipamentos, conforme **subitem 2.5.**, freqüência de 60 (sessenta) Hertz;

- As fontes de alimentação são redundantes por fontes internas independentes, com alimentação redundante;

de tal forma que, em caso de falha de uma das fontes por defeito ou por falta de alimentação elétrica em um dos 2 (dois) circuitos, o equipamento continue a funcionar sem prejuízo das aplicações.

OBS: Para confirmar as informações acima consulte os apêndice: x,y,z.....

Denial of Service in ISC BIND (srv bug)

General Affected External

General

Key Attributes

Attributes/Severity	**Medium Severity**
Vulnerability Type:	Network
Exploit Type:	Denial

Description
ISC BIND contains a Denial of Service vulnerability that can cause cause affected DNS servers running named to go into an infinite loop.

Consequences
If an SRV record is sent to the vulnerable name server, the server may be put into an infinite loop thereby preventing it from responding to further DNS requests.

Countermeasures
Update BIND to version 8.2.2-P7.

Access

Access Required:	None
Access Gained:	None

Discovery Date
13-NOV-2000

Affected Software and Programs

Software	Versions	Program	Versions
		BIND	8.2.x

External Advisories

Advisory Name	Advisory Source
CERT. Advisory CA-2000-20 Multiple Denial-of-Service Problems in ISC BIND>>Read	CERT

Links
Manufacturer

Related T
TAC Case
TAC Case
TAC Case
Dynamic (

BIND 8 Transaction Signature Buffer Overflow

General Affected External

General

Key Attributes

Attributes/Severity	**High Severity**
Vulnerability Type:	Network
Exploit Type:	Access

Description
BIND 8 improperly initializes buffers when processing error responses from transaction signatures without a valid key. The program assumes the buffer is set correctly when code for adding a new transaction signature is executed. This is a false assumption and will cause the stack or heap to overflow.

The overflow allows an attacker execute arbitrary code but placing it on the stack.

Consequences
Malicious users could compromise your DNS server with the same privilege as the running process. This process is usually run by root.

Countermeasures
Users of BIND 8 should upgrade to BIND 8.2.3 or BIND 9.1.

Access

Access Required:	Network Access to the DNS server.
Access Gained:	Access with the same privilege as the running process.

Discovery Date
29-JAN-2001

Affected

Affected Operating Systems

Operating System	Versions
Generic Unix	Any
Generic Linux	Any

Affected Software and Programs

Software	Versions	Program	Versions
BIND [PATCH]	Any	BIND	8.x.x

Affected Services

Name	Type	Ports	RPC
DNS	Info_status	53/TCP 53/UDP	

External

CVE Information

CVE ID: CVE-2001-0010

Advisories

Advisory Name	Advisory Source
CERT. Advisory CA-2001-02 Multiple Vulnerabilities in BIND>>Read	CERT
CERT. Advisory CA-2001-02 Multiple Vulnerabilities in BIND>>Read	CERT

Links

Fix

IP Overlapping Fragment Vulnerability

General Affected External

General

Key Attributes

Attributes/Severity	**Medium Severity**
Vulnerability Type:	Network
Exploit Type:	Denial

Description
Some implementations of the TCP/IP IP fragmentation re-assembly code do not properly handle overlapping IP fragments. On Microsoft Windows NT, this problem appears to be limited to ICMP packets. Teardrop and its derivations are a widely available attack tool that exploits this vulnerability.

Consequences
Unpatched systems are susceptible to denial of service attacks using the "teardrop," "teardrop2," "boink," and "bonk" attacks.

Countermeasures
The related CERT advisory lists patches or upgrades that fix this problem.

Microsoft regularly releases "hotfixes" between service pack updates. These hotfixes normally solve many problems at once and should be applied to vulnerable hosts. This fix is not included in service packs 3 and below and therefore needs to be applied separately. For Microsoft Windows NT, apply the teardrop2-fix patch available from Microsoft, which is available at the following URL: ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/NT40/hotfixes-postSP3/

NOTE: Please be sure to read ALL the Microsoft documentation on applying HotFixes. HotFixes are VERY installation-order dependent. Applying one hotfix out of order can wipe out multiple other patches.

Access
Access Required: network access
Access Gained:

Products
IDS Signature IP Fragments Overlap
SignatureId/ SubId 1103/0
CSID Versions: 2.1.1
Signature Description This signature identifies that two fragments contained within the same IP datagram have offsets that indicate that they share positioning within the datagram. This could mean that fragment A is being completely overwritten by fragment B, or that fragment A is partially being overwritten by fragment B. Some operating systems do not properly handle fragments that overlap in this manner and may throw exceptions or behave in other undesirable ways upon

	receipt of overlapping fragments. This is the basis for the so called teardrop Denial Of Service Attacks.
Alarm Level	5
Benign Triggers	Fragment overlaps could occur normally in network traffic due to retransmissions of datagrams. If a packet is retransmitted and the packet requires fragmentation the fragmentation may be performed differently if the packet takes a different route than the originally transmitted packet. Fragmented traffic is in itself unusual. Overlapping of fragments is rarely if ever seen. A large number of overlapping fragments is not to be expected at all, and is most probably an active attack.
Signature Type	NETWORK
Signature Structure	COMPOSITE
Implementation	CONTEXT

Scanner xxx
CSS Versions: 2.0

Affected
Affected Operating Systems

Operating System	Versions
Windows NT [PATCH]	Any
HP-UX [PATCH]	11.0,9.0
SunOS [PATCH]	4.1.4,4.1.3_U1
NetBSD [PATCH]	1.1
Cisco IOS [PATCH]on Cisco 7xx [PATCH]	Any
Caldera Linux [PATCH]	2.0.0,2.0.31

Affected Services

Name	Type	Ports	RPC
IP	Networking		

External
CVE Information
CVE ID: CVE-2000-0305

Advisories

Advisory Name	Advisory Source
CERT* Advisory CA-97.28>>Read	CERT

Aliases

Vendor	Product	Alias
Publicly Known Names	Public	Teardrop, Teardrop2, Boink, Bonk

TECHNICAL SUPPORT

Cisco Secure Encyclopedia

DNS Show Version

General

Key Attributes

Attributes/Severity	**Medium Severity**
Vulnerability Type:	Network
Exploit Type:	Recon

Description
If the DNS server reveals its version, an attacker can determine whether the server is likely to be vulnerable to exploitation.

Consequences
An attacker can determine if the DNS server is vulnerable to several common exploits and denial of service (DoS) attacks.

Countermeasures
Use the options statement in the BIND configuration file to restrict DNS queries including inverse and version information.

Access

Access Required:	None
Access Gained:	None

Products
IDS Signature DNS Version Request

SignatureId/ SubId	6054/0
CSID Versions:	2.2.1.5
Signature Description	Triggers when a request for the version of a DNS server is detected. Numerous versions of the popular BIND DNS server contain buffer overflow vulnerabilities, and scanners have been written to detect the presence of vulnerable DNS servers.
Alarm Level	3
Benign Triggers	No known triggers.
Signature Type	NETWORK
Signature Structure	ATOMIC
Implementation	CONTENT

Related Vulnerabilities

ID	Descriptive Name
1156	DNS Inverse Query Buffer Overflow
1133	DNS Reconnaissance Exploit
1318	BIND NXT Buffer Overflow

Statistics
Statistical Data - for Hosts with DNS service enabled

Industry Vertical	Percentage of Hosts with this Vulnerability		Percentage of Hosts with Service Vulnerable	
Perspective	**Internal**	**External**	**Internal**	**External**
Advanced Technology		1.75%		1.75%
Photography		16.67%		16.67%
Computers	33.02%	18.67%	43.30%	41.33%
Computers	47.39%	26.42%	63.03%	54.72%
Software	5.77%		5.77%	14.29%
Consumables	4.67%		4.67%	
Food/Beverage	4.67%		4.67%	
Financial Services	12.63%	4.94%	15.37%	4.94%
Banking	3.70%	3.85%	7.41%	3.85%
Finance	13.56%	5.22%	14.48%	5.22%
Insurance			61.54%	
Healthcare	54.95%		57.14%	52.17%
Healthcare			35.29%	55.81%
Pharmaceuticals	58.59%		58.59%	
Industrial		26.56%		34.38%
Building Materials				50.00%
Farm Equipment				100.00%
Industrial Equipment		31.48%		31.48%
Internet	25.00%	37.50%	32.14%	37.50%
Internet/Web	25.00%	37.50%	32.14%	37.50%
Other	3.85%	28.12%	3.85%	50.00%
International	3.85%		3.85%	37.50%
Unspecified		37.50%		54.17%
Public Sector	2.54%		19.85%	44.44%
Education	9.09%		9.09%	100.00%
Government	2.16%		20.49%	37.50%
Retail		16.67%		16.67%
Furniture		16.67%		16.67%
Service/Information	9.62%		53.85%	25.93%
Advertising	83.33%		83.33%	
Media/Entertainment				25.40%
Outsource Services				42.86%
Services			60.53%	
Utilities	10.91%	1.36%	24.00%	53.39%
ISP		2.38%		41.90%
Telco	20.55%		39.73%	75.69%
Utilities			23.53%	
Overall	**17.27%**	**5.93%**	**25.52%**	**34.87%**

Affected

Affected Operating Systems

Operating System	Versions
Windows NT [PATCH]	Any
Generic Unix	Any
Generic Linux	Any

Affected Software and Programs

Software	Versions	Program	Versions
BIND [PATCH]	8.x.x,4.x.x		

Affected Services

Name	Type	Ports	RPC
DNS	Info_status	53/TCP 53/UDP	

External

CVE Information

CVE ID: CVE-1999-0009

Advisories

Advisory Name	Advisory Source
Denial of Service (DoS) attacks using the Domain Name System (DNS)>>Read	AUSCERT
CA-99-14 Multiple Vulnerabilities in BIND>>Read	CERT

Links

General Information
Fix

Aliases

Vendor	Product	Alias
Security Focus	Vulnerabilities Database	ISC BIND named SIGINT and SIGIOT symlink Vulnerability
Security Focus	Vulnerabilities Database	Multiple Vendor BIND (NXT Overflow & Denial of Service) Vulnerabilities
Security Focus	Vulnerabilities Database	Multiple Vendor BIND iquery buffer overflow Vulnerability
ISS XForce	XForce Database	bind
ISS XForce	XForce Database	bind-axfr-dos
ISS XForce	XForce Database	bind-bo
ISS XForce	XForce Database	bind-dos
ISS XForce	XForce Database	bind-fdmax-dos
ISS XForce	XForce Database	bind-maxdname-bo
ISS XForce	XForce Database	bind-naptr-dos
ISS XForce	XForce Database	bind-nxt-bo
ISS XForce	XForce Database	bind-sigrecord-dos
ISS XForce	XForce Database	bind-solinger-dos
ISS XForce	XForce Database	bind-version
ISS XForce	XForce Database	bind-victim-domain-dos
ISS	XForce Database	tcp-port-bind

XForce
ISS
XForce

XForce Database udp-port-bind

Mars_NWE Buffer Overflow Vulnerability

General Affected External

General

Key Attributes

Attributes/Severity	**Medium Severity**
Vulnerability Type:	Host
Exploit Type:	Access

Description
There is no bounds checking in the setuid root components of Mars Netware package. This allows for buffer overflows that would return setuid root shells. Also, a local root compromise is possible if users create carefully designed directories and/or bindery objects.

Consequences
Possible root access

Countermeasures
Update the RPM package using the following command:

rpm -Fvh filename

where filename is one of the RPMs below.

Intel:

ftp://updates.redhat.com/6.0/i386/mars-nwe-0.99pl17-4.i386.rpm

Alpha:

ftp://updates.redhat.com/6.0/alpha/mars-nwe-0.99pl17-4.alpha.rpm

SPARC:

ftp://updates.redhat.com/6.0/sparcmars-nwe-0.99pl17-4.sparc.rpm

Source:

ftp://updates.redhat.com/6.0/SRPMS/mars-nwe-0.99pl17-4.src.rpm

Architecture neutral:

ftp://updates.redhat.com/6.0/noarch/

Access

Access Required:	User Access
Access Gained:	Root Access

Affected
Affected Operating Systems

Operating System	Versions
Redhat Linux [PATCH]on x86 [PATCH]	5.2,4.2
Redhat Linux [PATCH]	6.0

Affected Software and Programs

Software	Versions	Program	Versions
		mars_nwe [PATCH]	Any

Affected Services

Name	Type	Ports	RPC
application	Application		

External CVE Information

CVE ID: CVE-1999-0774

Advisories

Advisory Name	Advisory Source
Buffer overflow in mars_nwe>>Read	RedHat

Links

General Information
Exploit, Solution & Discussion

Aliases

Vendor	Product	Alias
Security Focus	Vulnerabilities Database	Mars NWE Buffer Overflow Vulnerabilities

TECHNICAL SUPPORT

Cisco Secure Encyclopedia

RPC Set/Unset Spoof

General Affected External

General

Key Attributes

Attributes/Severity	**High Severity**
Vulnerability Type:	Network
Exploit Type:	Denial

Description
The portmapper will allow systems that appear to come from localhost (i.e., a source address of 127.x.x.x) to register and unregister services. Since the portmapper allows the use of UDP, this is easily spoofed.

Consequences
This vulnerability can be exploited as a Denial of Service (DOS) to remove applications such as NFS and NIS from the portmapper. If the attacker has local access, they can start rogue daemons of their own creation.

Countermeasures
Do not allow packets with a source address of 127.x.x.x to reach your network. Upgrade to a patched version or run a secure portmapper.

Discovery Date
22-AUG-1999

Products

IDS Signature RPC Unset Spoof

SignatureId/ SubId	6105/0
CSID Versions:	2.2.1.1
Signature Description	This signature triggers when an RPC unset request with a source address of 127.x.x.x is detected.
Alarm Level	5
Benign Triggers	No known triggers.
Signature Type	NETWORK
Signature Structure	ATOMIC
Implementation	CONTENT

IDS Signature RPC Set Spoof

SignatureId/ SubId	6104/0
CSID Versions:	2.2.1.1
Signature Description	This signature triggers when an RPC set request with a source address of 127.x.x.x is detected.
Alarm Level	5
Benign Triggers	No known benign triggers exist for this signature.
Signature Type	NETWORK
Signature Structure	ATOMIC

Implementation CONTENT

Affected

Affected Operating Systems

Operating System	Versions
Solaris [PATCH]	Any

Affected Software and Programs

Software	Versions	Program	Versions
		portmapper	Any

Affected Services

Name	Type	Ports	RPC
RPC	File_sharing	111/TCP 111/UDP	rwall/100008 cmsd/100068 ttdbserverd/100083 sprayd/100012 rstatd/100001 amd/300019 ypbind/100007 yppasswd/100009 mountd/100005 pcnfsd/150001 amd/100065 portmapper/100000 rquotad/100011 selection_svc/100015 rexd/100017 YPServ/100004 ypupdated/100028 sadmind/100232 bootparam/100026

External

Aliases

Vendor	Product	Alias
ISS XForce	XForce Database	rpcbind-spoof

TECHNICAL SUPPORT

Cisco Secure Encyclopedia

Solaris rwalld String Format Command Execution

General

Key Attributes

Attributes/Severity	**High Severity**
Vulnerability Type:	Host
Exploit Type:	Access

Description
Certain versions of the Solaris operating system contain a string format vulnerability in the rwalld RPC service. rwalld is used to send system messages to all the users logged into a remote host by relaying those messages through the wall program.

Typically, rwalld is executed by the inetd super-daemon which results in rwalld executing with root privileges.

Consequences
Because rwalld is spawned by the inetd daemon, it executes with root privileges. A remote attacker who is able to properly inject arbitrary code to the rwalld daemon on the vulnerable system can execute arbitrary commands on the system as the root user.

Countermeasures
Apply the patches available at the referenced link to Sun. If this is not possible, comment out the service in /etc/inetd.conf and restart the inetd service.

Access

Access Required:	Network connectivity to the vulnerable system.
Access Gained:	Possible root access.

Discovery Date
30-APR-2002

Products
IDS Signature rwalld String Format

SignatureId/ SubId	6198/0
CSID Versions:	Any
Signature Description	This signature fires if an unusually long message is detected being sent to the RPC service rwalld. This may indicate a buffer overflow or string format attack has been attempted.
Alarm Level	5
Benign Triggers	This signature may fire while inspecting legitimate rwalld traffic, if the message sent is long. False positives can be reduced by adjusting the RpcMaxLength parameter to a larger value appropriate for your network.
Signature Type	NETWORK
Signature	

Structure COMPOSITE
Implementation CONTENT

Affected
Affected Operating Systems

Operating System	Versions
Solaris [PATCH]	2.5.1,2.6,7.0,8.0

Affected Software and Programs

Software	Versions	Program	Versions
rpcbind	Any	rpc.rwalld [PATCH]	Any

Affected Services

Name	Type	Ports	RPC
RPC	File_sharing	111/TCP 111/UDP	rwall/100008 cmsd/100068 ttdbserverd/100083 sprayd/100012 rstatd/100001 amd/300019 ypbind/100007 yppasswd/100009 mountd/100005 pcnfsd/150001 amd/100065 portmapper/100000 rquotad/100011 selection_svc/100015 rexd/100017 YPServ/100004 ypupdated/100028 sadmind/100232 bootparam/100026

External
Advisories

Advisory Name	Advisory Source
CA-2002-10 Format String Vulnerability in rpc.rwalld>>Read	CERT

Links
Exploit, Solution & Discussion

WinGate Remote File Access Vulnerability

General Affected External

General

Key Attributes

Attributes/Severity	**Medium Severity**
Vulnerability Type:	Network
Exploit Type:	Access

Description
WinGate is proxy/firewall web server software that allows a network to share a single Internet connection. The WinGate Log File service contains a vulnerability that will allow an attacker to read any file on the WinGate server. Although the default WinGate settings bind all services to the loopback address (127.0.0.1) and do not allow requests from the Internet, the WinGate administrator can change these settings.

Consequences
An attacker can read any file on the vulnerable WinGate system.

Countermeasures
Follow WinGate's recommended security measures (see the Links section for more details). The best safeguard is to allow only the localhost to view log files.

Access

Access Required:	network
Access Gained:	Read Files

Discovery Date
22-FEB-1999

Affected

Affected Operating Systems

Operating System	Versions
Windows 95 [PATCH]	Any
Windows NT [PATCH]	Any
Windows 98 [PATCH]	Any

Affected Software and Programs

Software	Versions	Program	Versions
		WinGate	3.0

Affected Services

Name	Type	Ports	RPC

Remote Access Other

External Advisories

Advisory Name	Advisory Source
AD02221999: Multiple WinGate Vulnerabilites>>Read	BUGTRAQ

Links

General Information
General Information
General Information

TECHNICAL SUPPORT
Cisco Secure Encyclopedia

TECHNICAL SUPPORT

Search:

Cisco Secure Encyclopedia

Quick Search: GO Advanced Search

Search A

Toolkit: F

Feedback

Related T
TAC Case
TAC Case
TAC Case
Dynamic (

BIND NXT Buffer Overflow

General Affected External

General

Key Attributes

Attributes/Severity	**High Severity**
Vulnerability Type:	Network
Exploit Type:	Access

Description
Berkeley Internet Name Domain (BIND) is an implementation of the Domain Name Service (DNS) protocol. It includes a name server called 'named'. Vulnerable versions of the named server fail to properly validate NXT responses, and are subject to buffer overflows.

Consequences
A remote attacker can crash the DNS service or execute arbitrary commands as root on the server.

Countermeasures
Upgrade to at least BIND 8.2.2 patch level 3.

Access

Access Required:	None
Access Gained:	None

Products
Scanner xxx
CSS Versions: 2.0.1.2
IDS Signature DNS NXT Buffer Overflow

SignatureId/ SubId	6056/0
CSID Versions:	2.2.1.4
Signature Description	This alarm triggers when a DNS server response arrives that has a long NXT resource where the length of the resource data is > 2069 bytes OR the length of the TCP stream containing the NXT resource is > 3000 bytes.
Alarm Level	5
Benign Triggers	No known triggers.
Signature Type	NETWORK
Signature Structure	COMPOSITE
Implementation	CONTENT

IDS Signature DNS SIG Buffer Overflow

SignatureId/ SubId	6057/0
CSID Versions:	2.2.1.4
Signature Description	This alarm triggers when a DNS server response arrives that has a long SIG resource where the length of the

resource data is > 2069 bytes OR the length of the TCP stream containing the SIG resource is > 3000 bytes.

Alarm Level	4
Benign Triggers	No known triggers.
Signature Type	NETWORK
Signature Structure	COMPOSITE
Implementation	CONTEXT

Affected

Affected Operating Systems

Operating System	Versions
Solaris [PATCH]	7.0
AIX [PATCH]	4.3.x
HP-UX [PATCH]	Any
SCO OpenServer [PATCH]	5.x.x
Unixware [PATCH]	7.x.x,2.x.x
Caldera Linux [PATCH]	2.3

Affected Software and Programs

Software	Versions	Program	Versions
BIND [PATCH]	8.2.1,8.2	named [PATCH]	8.2.1,8.2

Affected Services

Name	Type	Ports	RPC
BIND	Application	53/TCP 53/UDP	

External

CVE Information

CVE ID: CVE-1999-0833

Advisories

Advisory Name	Advisory Source
K-007: Multiple Vulnerabilities in BIND>>Read	CIAC
Multiple Vendor BIND (NXT Overflow & Denial of Service) Vulnerabilities >>Read	SecurityFocus

Links

General Information
Fix
Exploit

Aliases

Vendor	Product	Alias
ISS XForce	XForce Database	bind-nxt-bo(3476)

Cisco Systems

Technical Support GO

TECHNICAL SUPPORT
Cisco Secure Encyclopedia

TECHNICAL SUPPORT

Search:

Cisco Secure Encyclopedia

Search A

Quick Search: GO Advanced Search

Toolkit: F

Feedback

DNS Reconnaissance Exploit

General Affected Statistics External

General

Related T
TAC Case
TAC Case
TAC Case
Dynamic (

Key Attributes

Attributes/Severity	**Medium Severity**
Vulnerability Type:	Network
Exploit Type:	Recon

Description
The Domain Name Service (DNS) reports information for hosts in its domain. This information can be used for reconnaissance and targeting. Commands used for reconnaissance are HINFO, zone transfer (type 252), and request all records (type 255).

Consequences
An attacker can use DNS reconnaissance to map the entire network by discovering IP addresses of internal hosts.

Countermeasures
For Microsoft DNS:

To configure zone security, use the following procedure:
1. Choose Programs from the Start menu, choose Administrative Tools (Common), and then select DNS Manager.
2. Right-click on the primary zone icon from the Server list.
3. Click Properties.
4. Select the Notify tab.
5. In the Notify List, add the IP addresses of the secondaries that are allowed to access the primary.
6. Select the "Only Allow Access From Secondaries Included on the Notify List" checkbox.

For Linux/Unix DNS:

To configure zone security, append the following options statement to the BIND configuration file:

```
options {
[ allow-transfer { address_match_list }; ]
};
```

Access
Access Required: None
Access Gained: None

Discovery Date
01-DEC-1999

Products

IDS Signature DNS Request for All Records

SignatureId/ SubId	6053/0
CSID Versions:	2.1.1
Signature Description	Triggers on a DNS request for all records. Similar to a zone transfer in that it provides a method for transferring DNS records from a server to another requesting host. The primary difference is that all DNS records are transferred not just those specific to a particular zone. This is indicative that your network may be under reconnaissance.
Alarm Level	2
Benign Triggers	This is a normal transaction on networks. If the source of the request was not a secondary server on your network this may be a reconnaissance effort, and heightened awareness of future security relevant events is suggested.
Signature Type	NETWORK
Signature Structure	ATOMIC
Implementation	CONTENT

IDS Signature DNS Incremental zone transfer

SignatureId/ SubId	6063/0
CSID Versions:	Any
Signature Description	Alarms when a DNS query type of 251 is detected.
Alarm Level	2
Benign Triggers	Valid incremental zone transfers from secondary DNS servers may cause this alarm to fire.
Signature Type	NETWORK
Signature Structure	ATOMIC
Implementation	CONTENT

IDS Signature DNS authors request

SignatureId/ SubId	6062/0
CSID Versions:	Any
Signature Description	Alarms when a DNS query type TXT class CHAOS is detected with string "Authors.Bind" (case insensitive).
Alarm Level	3
Benign Triggers	No known triggers.
Signature Type	NETWORK
Signature Structure	ATOMIC
Implementation	CONTENT

Scanner xxx

CSS Versions: 2.0

IDS Signature DNS HINFO Request

SignatureId/ SubId	6050/0
CSID Versions:	2.1.1
Signature Description	Triggers on an attempt to access HINFO records from a DNS server. The Domain Name Service (DNS) includes an optional record type that allows for system information to be recorded and retrieved. This information typically includes the OS and hardware platform that the system is running on. There is very little utility in including this record in the database, and it provides attackers with valuable targeting information. It is suggested that this record not be included in your DNS database for this reason. This is indicative that your network may be under reconnaissance.
Alarm Level	3
Benign Triggers	This DNS information field may be accessed for many valid reasons from the network. Most likely curiosity on the part of a novice user or the a system administrator in search of all systems on the network running a particular operating system. Heighten awareness of future security relevant events as this may be a reconnaissance effort.
Signature Type	NETWORK
Signature	

Structure	ATOMIC
Implementation	CONTENT

IDS Signature DNS Zone Transfer

SignatureId/ SubId	6051/0
CSID Versions:	2.1.1
Signature Description	Triggers on normal DNS zone transfers, in which the source port is 53. Zone transfers are the method by which secondary DNS servers update their DNS records. All DNS records are transferred at once from the primary to secondary server. This transfers records only for the zone specified. This is indicative that your network may be under reconnaissance.
Alarm Level	1
Benign Triggers	This is a normal transaction on networks. If the source of the request was not a secondary server on your network this may be a reconnaissance effort, and heightened awareness of future security relevant events is suggested.
Signature Type	NETWORK
Signature Structure	ATOMIC
Implementation	CONTENT

IDS Signature DNS Zone Transfer from High Port

SignatureId/ SubId	6052/0
CSID Versions:	2.1.1
Signature Description	Triggers on an illegitimate DNS zone transfer, in which the source port is not equal to 53. Zone transfers are the method by which secondary DNS servers update their DNS records. All DNS records are transferred at once from the primary to secondary server. This transfers records only for the zone specified. Because of the access method this is indicative that your network most probably is under reconnaissance. This may be the prelude to more serious attacks.
Alarm Level	4
Benign Triggers	There are no benign triggers for this event. Zone transfers performed in this manner are observed only when there is an active attempt to hide the activity. This is most probably a reconnaissance effort and heightened awareness of future security relevant events is suggested.
Signature Type	NETWORK
Signature Structure	ATOMIC
Implementation	CONTENT

Statistics

Statistical Data - for Hosts with DNS service enabled

Industry Vertical	Percentage of Hosts with this Vulnerability		Percentage of Hosts with Service Vulnerable	
Perspective	**Internal**	**External**	**Internal**	**External**
Advanced Technology				1.75%
Photography				16.67%
Computers	0.62%	1.33%	43.30%	41.33%
Computers	0.95%	1.89%	63.03%	54.72%
Software			5.77%	14.29%
Consumables			4.67%	
Food/Beverage			4.67%	
Financial Services	0.84%		15.37%	4.94%
Banking			7.41%	3.85%
Finance	0.92%		14.48%	5.22%

Insurance			61.54%	
Healthcare			57.14%	52.17%
Healthcare			35.29%	55.81%
Pharmaceuticals			58.59%	
Industrial		3.12%		34.38%
Building Materials		50.00%		50.00%
Farm Equipment				100.00%
Industrial Equipment				31.48%
Internet			32.14%	37.50%
Internet/Web			32.14%	37.50%
Other		18.75%	3.85%	50.00%
International		25.00%	3.85%	37.50%
Unspecified		16.67%		54.17%
Public Sector		27.78%	19.85%	44.44%
Education		100.00%	9.09%	100.00%
Government		18.75%	20.49%	37.50%
Retail				16.67%
Furniture				16.67%
Service/Information			53.85%	25.93%
Advertising			83.33%	
Media/Entertainment				25.40%
Outsource Services				42.86%
Services			60.53%	
Utilities	0.73%	1.36%	24.00%	53.39%
ISP		2.38%		41.90%
Telco			39.73%	75.69%
Utilities	5.88%		23.53%	
Overall	**0.36%**	**1.91%**	**25.52%**	**34.87%**

Affected

Affected Operating Systems

Operating System	Versions
Windows NT [PATCH]	4.0,2000
Generic Unix	Any
Generic Linux	Any

Affected Software and Programs

Software	Versions	Program	Versions
BIND [PATCH]	8.x.x,4.x.x	DNS	8.x.x,4.x.x
NT Server [PATCH]	4.0	Domain Name Service [PATCH]	4.0

Affected Services

Name	Type	Ports	RPC
DNS	Info_status	53/TCP 53/UDP	

External Advisories

Advisory Name	Advisory Source
Microsoft DNS server may allow DNS zone transfer to any hosts>>Read	ISS
DNS Zone Transfers from high ports>>Read	ISS
DNS server inverse queries>>Read	ISS
DNS request made for all records>>Read	ISS
DNS honors zone transfer requests>>Read	ISS
DNS HInfo request decode>>Read	ISS

Links

Fix
General Information
General Information

Aliases

Vendor	Product	Alias
ISS XForce	XForce Database	nt-ms-dns-zone-xfer
ISS XForce	XForce Database	decod-dns-zone
ISS XForce	XForce Database	dns-zonexfer
ISS XForce	XForce Database	decod-dns-hinfo
ISS XForce	XForce Database	dns-iquery
ISS XForce	XForce Database	decod-dns-all

Multiple Vulnerabilities in BIND v4 and v8

General Affected External

General

Key Attributes

Attributes/Severity	**High Severity**
Vulnerability Type:	Network
Exploit Type:	Access

Description
There exists multiple vulnerabilities in ISC BIND version 4 and version 8. These vulnerabilities could allow remote users to gain root access to the machine running BIND.

Environment Variable Disclosure vulnerability:
ISC BIND contains a vulnerability that can allow a remote attacker to access the program stack, which could expose program and/or environment variables. This vulnerability affects both BIND 4 and BIND 8, and can be triggered by sending a specially formatted query to vulnerable BIND servers.

Data validation error in nslookupComplain():
The vulnerability exists in all BIND versions prior to 4.9.8. The buffer overflow exists in a local character array used to create an error message sent to syslog. A carefully crafted DNS query could disrupt normal operations with the result either being a denial of service or remote execution of arbitrary code.

Buffer overflow in Transaction Signature:
There is a problem with transaction signatures in BIND 8. During the processing, BIND checks signatures for valid keys. If a transaction signature is found without a valid key, the code will perform an error response which fails to initialize buffers appropriately. The program assumes the buffer is set correctly when code for adding a new transaction signature is executed. This is a false assumption and will cause the stack or heap to overflow.

Buffer overflow in nslookupComplain():
The vulnerability exists in all BIND versions prior to 4.9.8. The buffer overflow exists in a local character array used to create an error message sent to syslog. A carefully crafted DNS query could disrupt normal operations with the result either being a denial of service or remote execution of arbitrary code.

Consequences
As soon as exploits become widely available, attackers will start using this vulnerability to gain root access on every nameserver they can find.

Countermeasures
CERT recommends that users of BIND 4.9.x or 8.2.x upgrade to the newly released BIND 4.9.8 or BIND 8.2.3, respectively.

Access

Access Required:	network
Access Gained:	root

Discovery Date
29-JAN-2001

Products
Scanner
CSS Versions: 2.0.2.3

IDS Signature DNS TSIG Overflow

SignatureId/ SubId	6059/0
CSID Versions:	Any
Signature Description	Alarms when a DNS query type TSIG is detected and the domain name is greater than 255.
Alarm Level	5
Benign Triggers	No known triggers.
Signature Type	NETWORK
Signature Structure	ATOMIC
Implementation	CONTENT

IDS Signature DNS complain overflow

SignatureId/ SubId	6060/0
CSID Versions:	Any
Signature Description	Alarms when an NS record is detected with a domain name greater than 255 and the IP address is 0.0.0.0, 255.255.255.255 or a multicast of form 224.X.X.X
Alarm Level	5
Benign Triggers	No known triggers.
Signature Type	NETWORK
Signature Structure	ATOMIC
Implementation	CONTENT

IDS Signature DNS infoleak

SignatureId/ SubId	6061/0
CSID Versions:	Any
Signature Description	Alarms when a DNS IQUERY is detected with a record data Length greater than 4 and Class IN.
Alarm Level	4
Benign Triggers	No known triggers.
Signature Type	NETWORK
Signature Structure	ATOMIC
Implementation	CONTENT

Affected Software and Programs

Software	Versions	Program	Versions
BIND [PATCH]	Any,Any		

Affected Services

Name	Type	Ports	RPC
BIND	Application	53/TCP 53/UDP	

External Advisories

Advisory Name	Advisory Source
COVERT-2001-01 >>Read	NAI COVERT Labs
CA-2001-02 Multiple Vulnerabilities in BIND >>Read	CERT

Links
General Information
General Information
General Information

General Information
General Information
General Information
General Information

ESL9595L2

A tape library ESL9595L2 possui características que permitem uma alta disponibilidade do ambiente.

Os drives podem ser substituídos online sem parada do servidor ou da aplicação. O dado é automaticamente redirecionado através de outros drives sem necessidade de reconfiguração.

Para manter alta disponibilidade, várias ferramentas de diagnóstico podem prover um rápido isolamento e recuperação de problemas de hardware, incluindo testes no power-on do equipamento.

A limpeza automática do drive aumenta a disponibilidade e elimina a necessidade de manutenção preventiva e seu downtime associado.

A tape library possui componentes redundantes como fontes, ventiladores e PDUs.

Para manter a disponibilidade do ambiente e operação contínua, os drives são hot-

pluggable e as fontes e ventiladores hot-swappable.

Outras informações sobre disponibilidade da tape library ESL9595L2 podem ser obtidas nos catálogos que foram anexados na proposta.

Descrição das Tapes Library

BRASILIA

2 (duas) Hp StorageWorks ESL9595 com:
400 Slots,
20 drives ultrium 460,
5 bridges modelo e2400-160 FC com 20 canais SCSI
1 (um) Pass-through para conecção das ESL9595

SAN Switch

4 (quatro) HP StorageWorks Core Switch 2/64 postas

São Paulo

1 (uma) Hp storageworks ESL9595 com:
400 Slots,
12 drives Ultrium 460,
3 bridges modelo e2400-160 FC com 12 canais SCSI

SAN Switch

2 (dois) HP StorageWorks Core Switch 2/64 portas

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 1.2 of Security Monitor introduces several new features and support for Security Agent MC servers.

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.

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 Detection 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.

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.

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.

78-15663-01

New Features in Monitoring Center for Security (Security Monitor) Version 1.2

The following new features have been added to Security Monitor version 1.2:

- Support for Security Agent MC servers. You can receive alarm data from a Security Agent MC server, view the alarms in the Event Viewer, and generate reports based on those alarms.
- Firewall reports. You can generate reports based on firewall events.
- Event Viewer enhancements. You can save your customized column order in Event Viewer.
- Expanded data export and import. You can import data from and export data to NrLog, IDIOM, and pruning archive files.
- Database compact. You can reclaim disk space with the database compact utility.

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 the following report types:

- **Audit Reports**—Provide information about system events.
- **Firewall Reports**—Provide information about Firewall events.
- **CSA Reports**—Provide information about events generated by Management Center for Cisco Security Agents (Security Agent MC).

Refer to the following topics for more information about defining and viewing reports:

Understanding the Types of Reports

You can view four categories of reports in Security Monitor: alarm reports, audit reports, CSA reports, and Firewall reports. Alarm reports provide information about the events being collected by Security Monitor. Audit reports provide information about Security Monitor system events. CSA reports provide information about Security Agent MC events. Firewall reports provide information about Firewall events.

Reports can be generated on-demand or scheduled for a later date and time. You can configure scheduled reports to repeat at regular intervals.

About Alarm Reports

You can generate the following alarm reports in Security Monitor:

- **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.

- **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.

- **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.

- **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 CSA Reports

You can generate the following reports for Security Agent MC events in Security Monitor:

- **CSA Summary Report**—Filterable by Alert Level and Time/Date.
- **CSA Alerts By Severity**—Filterable by Alert Level and Time/Date.
- **CSA Alerts By Group**—Filterable by Alert Level, Time/Date and Rule.
- **CSA Administration Event Summary**—Filterable by Alert Level and Time/Date.

About Firewall Reports

You can generate the following Firewall reports in Security Monitor:

- **User Activity Summary**—Summarizes the activities of all users who have made service requests through the selected Firewall within the specified time period. Filterable by Time/Date and Firewall Address.
- **Network Traffic Summary**—Summarizes all activities based on the service requests made through the selected Firewall within the specified time period. Filterable by Time/Date and Firewall Address.

- **Most Active Users**—Lists the users who have made the most service requests through the selected Firewall within the specified time period. This report provides statistics for up to N (defaults to 20) users. Filterable by Time/Date, Firewall Address, and Top N.
- **Most Accessed Web Sites**—Lists the HTTP sites that users who request services through the selected Firewall have accessed the most within the specified time period. This report provides statistics for up to N (defaults to 20) sites. Filterable by Time/Date, Firewall Address, and Top N.
- **Event Summary Report**—Summarizes the security, warning, and informational events that the selected Firewall has experienced within the specified time period. Filterable by Time/Date and Firewall Address.
- **Detailed User Activity**—Describes the full activities of all network session transactions that a specific user has conducted through the selected Firewall within the specified time period. It presents the full list of network sessions that have occurred within the time period. Filterable by Time/Date and Firewall Address.
- **Detailed Network Traffic**—Provides transaction information about a network service's sessions that transpire during a given time interval. For example, you can generate reports about HTTP on port 80, SSL on port 443, or DNS on port 53. To generate a detailed service report, you must configure the Firewall to enable logging of statistical events for the network service. Filterable by Time/Date, Firewall Address, and Service.
- **Denied Message Activity**—Lists all syslog messages for denied connections sent out by the Firewall within the specified time period. You can filter which types of deny messages appear in the report such as VPN, Attack, and AAA and ACL. Filterable by Time/Date, Firewall Address, and Denied Events.
- **Denied Connection Activity**—Lists all TCP, UDP, and ICMP messages for denied connections sent out by the Firewall for the specified time period. Filterable by Time/Date and Firewall Address.
- **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.

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.

To generate a report, follow these steps:

Step 1 Select **Reports > Generate**.

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**.

The Report Filtering page appears.

Step 3 Enter the report parameters for the report type you selected. Then, click **Next**.

The Schedule Report page appears.

Step 4 Enter a name for the report in the Report Title field.

Step 5 To export the generated report to an HTML file, select the **Export to** check box. Then, specify the exact path to the file that is to contain the generated report. The path should include the filename and the desired extension; for example, **/<dir>[/<dir>/[...]]/<filename>[.<ext>]**. No extension is appended to the filename if you do not specify an extension.

Step 6 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 7 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**.

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.

Viewing Reports

After you generate a report, you can view it.

Tip To understand how data is sorted in a report, refer to the numbers that appear in the column headings of the generated report. These numbers represent the sort keys. For example, data is sorted first based on the data in the column with a (1) in it, followed by the data in the column with a (2) in it, and so on.

To view a report, follow these steps:

Step 1 Select **Reports > View**.

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**.

The report appears in the Report page.

Step 4 To view the report in a new browser window, click **Open in Window. . .**.

The report appears in a new browser window.

Saving a Generated Report as an HTML File

After you generate a report, you can save the report as an HTML file.

To save a generated report as an HTML file, follow these steps:

Step 1 Select **Reports > View**.

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 To select the report that you want to export, select the check box corresponding to the report title.

Step 3 Click **Open in Window**.

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**.

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**.

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**.

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 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.

A check mark appears next to each report you selected.

Step 3 To delete the selected report, click **Delete**.

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**.

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.

A check mark appears next to the report you selected.

Step 3 To open the selected report template, click **Edit**.

A new page displays the report parameters. Depending on the type of report, the parameters are different.

Step 4 Change any report parameters that you want to. To save your changes, click **Finish**.

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**.

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.

A check mark appears next to each report you selected.

Step 3 To delete the report template, click **Delete**.

The selected report template and all associated end reports are deleted.

Windows 2000 Encrypting File System Vulnerability

General Affected External

General

Key Attributes

Attributes/Severity	**Low Severity**
Vulnerability Type:	Host
Exploit Type:	Access

Description
The default configuration of the Encrypting File System (EFS) for Microsoft Windows NT 2000 contains a vulnerability that can enable access to all encrypted data on a Windows NT 2000 workstation or server if physical access to the hardware can be obtained. No user accounts or passwords are required for this access. An administrator would have had to choose not to export their certificates or encrypt the registry. Access to the encrypted data is possible on standalone and domain member devices. This would include Windows 2000 workstations that are members of a domain as well as Windows 2000 resource/member servers that are in workgroups or domains. Access is also possible on Domain Controllers running Microsoft Active Directory Services (ADS).

Consequences
This vulnerability makes it possible to gain access to all encrypted data on a Windows NT 2000 workstation or server if physical access to the hardware can be obtained.

Countermeasures
To keep your data secure, you should export your certificates and/or use SysKey to Encrypt your registry. Physical security needs to be enforced for the critical stand-alone or domain controllers.

Access
Access Required: Local
Access Gained: Read encrypted files

Discovery Date
25-JUL-1999

Affected
Affected Operating Systems

Operating System	Versions
Windows 2000 [PATCH]	Any,Any,Any

Affected Software and Programs

Software	Versions	Program	Versions
		Encrypting File System (EFS) [PATCH]	Any

Affected Services

Name	Type	Ports	RPC
Non specific	Other		

External Advisories

Advisory Name	Advisory Source
CAN-2000-0420>>Read	CVE Candidate
ISS SAVANT Advisory 00/26>>Read	BUGTRAQ
Cracking Win2K EFS -- Whitepaper>>Read	BUGTRAQ
Microsoft Windows 2000 Default SYSKEY Configuration>>Read	BUGTRAQ

Links

Fix
Exploit

Aliases

Vendor	Product	Alias
ISS XForce	XForce Database	win2k-syskey-default-configuration

TECHNICAL SUPPORT
Cisco Secure Encyclopedia

TECHNICAL SUPPORT

Cisco Secure Encyclopedia

Quick Search: GO Advanced Search

Toolkit: F

Feedback

IIS Long URL Crash Bug

General Affected External

General

Key Attributes

Attributes/Severity	**Medium Severity**
Vulnerability Type:	Network
Exploit Type:	Denial

Description
A vulnerability in Microsoft Internet Information Server (IIS) version 2.0 and 3.0 running on Windows NT 4.0 allows users to locally or remotely cause an access violation on the Web server. As a result, the server crashes and is therefore rendered unresponsive until rebooted. Exploit code that sends requests of varying sizes (lengths) to the target IIS server is publicly available. Through this "trial and error," the code will eventually send the exact size request needed to render the target server unresponsive.

Consequences
An attacker could cause a Denial-of-Service (DoS), by crashing the web server and denying service to legitimate users. An administrator is required to reboot the server to restart Web services.

Countermeasures
1. Apply the Microsoft patch for this vulnerability.

2. Apply Windows NT Service Pack 4 or higher.

3. Upgrade to the latest version of Internet Information Server (IIS).

Discovery Date
27-JUN-1997

Products
IDS Signature IIS Long URL Crash Bug

SignatureId/ SubId	3220/0
CSID Versions:	2.1.1
Signature Description	This triggers when a large URL has been passed to a web server in an attempt to crash the system.
Benign Triggers	No known triggers.
Signature Type	NETWORK
Signature Structure	COMPOSITE
Implementation	CONTENT

Scanner xxx
CSS Versions: 2.0

Affected
Affected Operating Systems
Operating System Versions

Related T
TAC Case
TAC Case
TAC Case
Dynamic (

Windows NT [PATCH]	4.0

Affected Software and Programs

Software	Versions	Program	Versions
Internet Information Server (IIS) [PATCH]	2.0,3.0		

Affected Services

Name	Type	Ports	RPC
HTTP	Web	80/TCP 8080/TCP	

External CVE Information

CVE ID: CVE-1999-0281

Advisories

Advisory Name	Advisory Source
H-77: Microsoft IIS Boundary Condition Vulnerability>>Read	CIAC

Links

Exploit
General Information
Fix

Aliases

Vendor	Product	Alias
ISS XForce	XForce Database	http-iis-longurl

TECHNICAL SUPPORT

Cisco Secure Encyclopedia

Quick Search: GO Advanced Search

Toolkit: F

Feedback

AIX adb vulnerability

General Affected External

General

Key Attributes

Attributes/Severity	**Medium Severity**
Vulnerability Type:	Host
Exploit Type:	Denial

Description
The adb debugger shipped with IBM AIX versions 4.2.x and 4.3.x (including version 4.3.2) contains a vulnerability that can allow a malicious local user to shut down the operating system.

Consequences
A local user can shut down the operating system.

Countermeasures
A temporary fix is available via anonymous ftp from:
ftp://aix.software.ibm.com/aix/efixes/security/adb_hang.tar.Z

As noted in the Bugtraq post, this temporary fix has not been fully regression tested. The fix consists of a multiprocessor kernel that can be used on either a uniprocessor or multiprocessor machine. There may be a slight performance penalty when using a multiprocessor kernel on a uniprocessor machine.

For instructions on installing this fix, please refer to the Fix links.

Access
Access Required: user access
Access Gained:

Affected
Affected Operating Systems

Operating System	Versions
AIX [PATCH]	4.2.x,4.3.x

Affected Software and Programs

Software	Versions	Program	Versions
		adb debugger	Any

Affected Services

Name	Type	Ports	RPC
Non specific	Other		

External
CVE Information
CVE ID: CVE-1999-0694

Advisories

Advisory Name	Advisory Source
AIX adb vulnerability>>Read	IBM

Links
General Information
Fix
Fix

Aliases

Vendor	Product	Alias
Security Focus	Vulnerabilities Database	AIX adb Vulnerability

TECHNICAL SUPPORT
Cisco Secure Encyclopedia

TECHNICAL SUPPORT

Cisco Secure Encyclopedia

Quick Search: GO Advanced Search

sadmind RPC Buffer Overflow

General Affected External

General

Key Attributes

Attributes/Severity	**High Severity**
Vulnerability Type:	Network
Exploit Type:	Access

Description
The sadmind program is included with the default installation of Solaris 7, 2.6, 2.5.1, 2.5, 2.4, and 2.3. It is also included with SunOS 5.7, 5.6, 5.5.1, 5.5, 5.4, and 5.3. This program is used to perform remote system administration. A buffer overflow vulnerability has been found in the sadmind program which could lead to ROOT compromise of the host system.

A network worm has been discovered which exploits the sadmind RPC buffer overflow. The worm, upon a successful penetration of a Solaris system, will install tools which scan for and attack vulnerable IIS 4.0 and 5.0 web servers using a variant of the Unicode exploit. As a result, the main web page of the victimized web server is defaced.

Consequences
An attacker could exploit this vulnerability to execute arbitrary code with root privileges. As a result, the host system could be compromised.

Countermeasures
Apply the patch referenced in Sun Security Bulletin, #00191. Disable the sadmind service if it is not needed by killing the "sadmind" process and removing it from /etc/inetd.conf.

Access

Access Required:	Remote
Access Gained:	Root

Discovery Date
24-JUN-1999

Products
IDS Signature sadmind RPC Buffer Overflow

SignatureId/ SubId	6194/0
CSID Versions:	2.2.1.3
Signature Description	This signature fires when a call to RPC program number 100232 procedure 1 with a UDP packet length > 1024 bytes is detected.
Alarm Level	5
Benign Triggers	No known triggers.
Signature Type	NETWORK

Signature

Structure ATOMIC
Implementation CONTENT
Scanner xxx
CSS Versions: 2.0.1.2

Related Vulnerabilities

ID	Descriptive Name
2965	IIS Unicode Remote Command Execution

Affected
Affected Operating Systems

Operating System	Versions
Solaris [PATCH]	2.5.1,2.6,2.5,2.3,2.4,7.0
SunOS [PATCH]	5.5.1,5.6,5.4,5.7,5.5,5.3

Affected Software and Programs

Software	Versions	Program	Versions
		rpc.admind	Any

Affected Services

Name	Type	Ports	RPC
RPC	File_sharing	111/TCP 111/UDP	rwall/100008 cmsd/100068 ttdbserverd/100083 sprayd/100012 rstatd/100001 amd/300019 ypbind/100007 yppasswd/100009 mountd/100005 pcnfsd/150001 amd/100065 portmapper/100000 rquotad/100011 selection_svc/100015 rexd/100017 YPServ/100004 ypupdated/100028 sadmind/100232 bootparam/100026

External
CVE Information
CVE ID: CVE-1999-0977

Advisories

Advisory Name	Advisory Source
Buffer Overflow in Sun Solstice AdminSuite Daemon sadmind>>Read	CERT
CA-2001-11 sadmind/IIS Worm>>Read	CERT
Solaris sadmind Buffer Overflow Vulnerability>>Read	BUGTRAQ
Solaris Solstice AdminSuite (sadmind) daemon buffer overflow>>Read	ISS
K-013: Buffer Overflow in Sun Solstice AdminSuite Daemon sadmind>>Read	CIAC

Links
Fix
General Information

Aliases

Vendor	Product	Alias
Security Focus	Vulnerabilities Database	Solaris sadmind Buffer Overflow Vulnerability
ISS XForce	XForce Database	sol-sadmind-amslverify-bo

Cisco Secure Encyclopedia

Quick Search: GO Advanced Search

Corel Linux Update PATH

General Affected External

General

Key Attributes

Attributes/Severity	**Medium Severity**
Vulnerability Type:	Host
Exploit Type:	Access

Description
The "get_it" program of the "Corel Update" utility distributed with Corel's Linux OS contains a local PATH vulnerability, making it possible to spawn an arbitrary program with inherited root privileges, because the program (which is X based) runs as root.

Consequences
A non-root user can get root on the machine.

Countermeasures
1. Do not run the get_it program as setuid bit set.
2. Change the program to use absolute paths. However Corel did not release an official patch yet.

Access

Access Required:	local
Access Gained:	root

Discovery Date
12-JAN-2000

Affected

Affected Operating Systems

Operating System	Versions
Corel Linnux [PATCH]on x86 [PATCH]	Any

Affected Software and Programs

Software	Versions	Program	Versions
		get_it [PATCH]	Any

External

CVE Information
CVE ID: CVE-2000-0048

Links
Exploit, Solution & Discussion

Aliases

Vendor	Product	Alias
Security Focus	Vulnerabilities Database	Corel Linux get_it PATH Vulnerability
ISS XForce	XForce Database	linux-corel-update

BUSINESS STRATEGIES & SOLUTIONS | NETWORKING SOLUTIONS & PROVISIONED SERVICES | P
TECHNOLOGIES | ORDERING | TECHNICAL SUPPORT | LEARNING & EVENTS | PARTNERS & RESEL
Home | Logged In | Profile | Contacts & Feedback | Site Help

Cisco Systems

Technical Support GO

TECHNICAL SUPPORT
Cisco Secure Encyclopedia

TECHNICAL SUPPORT

Search:

Cisco Secure Encyclopedia

Search A

Quick Search: GO Advanced Search

Toolkit: F

Feedback

Root access via Remote Watch port

General Affected External

General

Related T
TAC Case
TAC Case
TAC Case
Dynamic (

Key Attributes

Attributes/Severity	**High Severity**
Vulnerability Type:	Network
Exploit Type:	Access

CSEC Common Name

Description
HP's Remote Watch system administration for HP-UX version 9.x allows unauthenticated root access. An attacker could execute commands as root by telneting to port 5556.

Consequences
Remote users could execute commands as root.

Countermeasures
HP advises that Remote Watch is an obsolete service and they recommend stopping and uninstalling this service from the host.

Access

Access Required:	None
Access Gained:	root

Discovery Date
24-OCT-1996

Affected
Affected Operating Systems

Operating System	Versions
HP-UX [PATCH]	9.x

Affected Services

Name	Type	Ports	RPC
Remote Watch	Net_management	5556/TCP	

External
Advisories

Advisory Name	Advisory Source
Vulnerabilities in HP Remote Watch Software>>Read	AUSCERT

Links
General Information

Aliases

Vendor	Product	Alias

ISS XForce hp-
XForce Database remote

Documentation

CISCO SYSTEMS

CiscoWorks

Network management solutions for enterprise LANs,WANs, VPNs, ISPs, campuses, and more. Documents include bundle installation information

---

- CiscoWorks Solutions
  Network management of LANs, WANs, VPNs, ISPs, campuses, and more. Documents include bundle installation information.
- CiscoWorks 1105
- CiscoWorks Small Network Management Solution
  Network management for the small network
- CiscoWorks VoIP Health Monitor
  Manages voice-specific devices in a network
- CiscoView (Standalone)
- Access Client/Server Software
- ACL Manager
  Access control list management on Cisco routers and Catalyst switches as an add-on to Resource Management Essentials
- Campus Manager
  Web-based network management tools that provide graphical views of network topology and end-user information
- CD One (includes CiscoView)
  Enables CiscoWorks management applications. CiscoView is the basic management tool for Cisco devices.
- CD Two
  Most inventory functions of Resource Management Essentials
- Cisco Secure Policy Manager
  Policy-based management of Cisco Secure PIX Firewalls and IOS Routers running Cisco Secure Integrated Software and Cisco Secure Integrated VPN Software
- Cisco Voice Manager
  Voice port configuration and management, and implementation of dial plans on voice-enabled Cisco routers
- Device Fault Manager
  Data fault analysis for Cisco devices

- Internetwork Performance Monitor
  Network response time and availability troubleshooting application
- Management Engine 1100 Series
  Service-level agreement (SLA) metric collection for SLA conformance reports
- NetScout nGenius Real-Time Monitor
- QoS Policy Manager
  Intelligent traffic management and resource utilization optimization across your enterprise network
- Resource Manager Essentials
  Device tracking with network monitoring and fault data, deployment for software images, and configuration displays for Cisco routers and Catalyst switches
- Service Level Manager
  Service-level contract management and implementation of service-level agreements (SLAs) for service providers
- User Registration Tool
- Voice Health Monitor
  Manages the voice-specific devices in a network
- VPN Monitor
  Virtual Private Network LAN-to-LAN and remote-access monitoring and troubleshooting
- CiscoWorks Common Services
- IDS Host Sensor Console
- Auto Update Server
- Management Center for IDS Sensors
- Management Center for Firewalls
- Management Center for VPN Routers
- Monitoring Center for Security
- Network Connectivity Monitor

HOME CONTENTS PREVIOUS NEXT GLOSSARY FEEDBACK SEARCH HELP

COBRA TECNOLOGIA
Integradora de Soluções em TI e Serviços

23/04/14

ANEXO ROTEADOR TIPO 01
PARTE 1

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls: 0329
3685
Doc:

COBRA Tecnologia S.A.
Estrada dos Bandeirantes 7966
CEP 22783-110 Rio de Janeiro RJ
Tel 21 2442-8800
www.cobra.com.br

ROTEADOR TIPO 1

ATRIBUTO	REQUISITOS DO EDITAL	ATRIBUTOS OFERTADOS	ATRIBUTOS OFERTADOS ADICIONALMENTE	CONFIRMA ATENDIMENTO (SIM / NÃO)	PÁGINA DA DOCUMENTAÇÃO TÉCNICA
1 - Router	Possuir estrutura de Chassis modular com pelo menos 04 slots para inserção de módulos e interfaces	Rack-mountable chassis - 04 slots para módulos de rede	N/A	SIM	Anexo 17 - pág. 1, 2 e 3
	Deverá ser montado em Rack de 19¨	Montável em Rack de 19¨	Pode ser montado opcionalmente em Rack de 23	SIM	Anexo 17 - pág. 3, 11
2 - Processamento	Possuir capacidade de roteamento de pelo menos 225.000 pps utilizando pacotes de 64 bytes	Performance de 225 Kpps	N/A	SIM	Anexo 17 - pág. 11 Ver Carta do Fabricante
3 - Interfaces	Possuir no mínimo 03 interfaces 10/100TX, fast Ethernet, Full Duplex, para cabos UTP categoria 5, com conectores tipo RJ-45	02 portas 10/100 integradas + 01 porta no módulo NM-1FE2W	N/A	SIM	Anexo 17 - pág. 3 e Anexo 18 - pág. 3
	Possuir no mínimo 08 interfaces síncronas V.35 de alta velocidade (atpe 2Mbps)	Foram colocados 02 cartões tipo WIC-2T, cada um com duas portas de WAN, perfazendo um total de 08 portas	N/A	SIM	Anexo 17 - pág. 2 e Anexo 19 - pág. 3
	Possuir no mínimo 02 interfaces ATM E3, compatível com o padrão ITU-T G703	Conforme Edital	N/A	SIM	Anexo 17A - pág. 5
	Possuir no mínimo 01 interface Gigabit Ethernet 1000BaseT	Foi colocada uma porta tipo GBIC, part-number WS-G5483	N/A	SIM	Ver propostas Técnica e Comercial
	Possuir MTBF de pelo menos 50.000 horas	Conforme Edital	N/A	SIM	Ver Carta do Fabricante
	Permitir o gerenciamento através de aplicação gráfica	Conforme Edital	N/A	SIM	Ver propostas Técnica e Comercial (Softwares de Gerenciamento)

Implementar o protocolo SNMP, incluindo a geração de traps	Conforme Edital	N/A	SIM	Anexo 19B - pág. 14 Anexo 19C (todas as páginas)
Gerenciável através do protocolo SNMP, com suporte a MIB II, conforme RFC 1213	Conforme Edital	N/A	SIM	Anexo 19D - pág. 10
Possuir descrição completa da MIB implementada no equipamento, inclusive as extensões privadas se existirem	Conforme Edital	N/A	SIM	Anexo 19D - pág. 5, 7, 8, 9, 10
Implementar TELNET para acesso a interface da linha de comando	Conforme Edital	N/A	SIM	Anexo 19D - pág. 12
Implementar protocolo SSH	Conforme Edital	N/A	SIM	Anexo 19B - pág. 13
Possuir proteção contra ataques de Denial of Services do tipo TCP SYN attack	Conforme Edital	N/A	SIM	Anexo 19E (todas as páginas)
Implementar IPSec padrão IETF com criptografia Triple DES	Todos os exigidos	AES (Advabced Encryption Standard)	SIM	Anexo 17 - pág. 5
Suporte para SYSLOG externo que deverá ser dimendionado e fornecido em hardware à parte	Conforme Edital	N/A	SIM	Anexo 17 (todas as páginas) Anexo 19D (todas as páginas) Anexo 19 (todas as páginas) Anexo 19H (todas as páginas)
Permitir a atualização de softwares utilizados no equipamento, através da Rede	Todos os exigidos	N/A	SIM	Anexo 19F (todas as páginas)
Implementar mecanismo de autenticação para acesso ao equipamento, baseado em servidor de autenticação / autorização do tipo RADIUS ou TACACS	Conforme Edital	N/A	SIM	Anexo 19B - pág. 12, 15

4 - Geral	Proteger a interface de comando do equipamento, através de senha	Conforme Edital	N/A	SIM	Anexo 19 (todas as páginas) Anexo 19B (todas as páginas) Anexo 19D (todas as páginas) Anexo 19H (todas as páginas)
	Implementar o potocolo VRRP ou similar, em todas as interfaces disponibilizadas	Conforme Edital	N/A	SIM	Anexo 19B - pág. 15
	Implementar o protocolo PIM para roteamento de Multicast	Conforme Edital	N/A	SIM	Anexo 19B - pág. 11
	Implementar roteamento IP usando os protocolos OSPF, RIP, RIP II e BGP4	Conforme Edital	N/A	SIM	Anexo 19D (todas as páginas)
	Implementar DHCP	Conforme Edital	N/A	SIM	Anexo 19B - pág. 3, 4
	Permitir a configuração de pelo menos 1024 rotas estáticas	Conforme Edital	N/A	SIM	Ver Carta do Fabricante
	Implementar Pollicy-based routing	Conforme Edital	N/A	SIM	Anexo 19I (todas as páginas)
	Implementar filtros para redistribuição de rotas entre RIP, OSPF e BGP4	Conforme Edital	N/A	SIM	Anexo 19B - pág. 2, 11, 12 - Anexo 19G (todas as páginas)
	Implementar as seguintes características para o protocolo BGP4: Route Reflectors, Route Confederations, Route Aggregation, IGP Synchronization e Route Flap Dampening	Conforme Edital	N/A	SIM	Anexo 19H (todas as páginas)
	Permitir a configuração de Policy-based routing baseado no endereço de origem da rede	Conforme Edital	N/A	SIM	Anexo 19I (todas as páginas)

	Suporta a implementação de NAT	Conforme Edital	N/A	SIM	Anexo 19B - pág. 10
	Deverá suportar inserção em rede com servidores de VOIP e VOFR	Conforme Edital	N/A	SIM	Anexo 19B - pág. 16
	Deverá suportar os protocolos G.711 e G.729 para o tráfego de voz e funcionar como Gateway H.323	Conforme Edital	N/A	SIM	Anexo 19B - pág. 6 Anexo 19J - pág. 1, 7, 8
	Servidores adicionais para instalação da gerência	Conforme Edital	N/A	SIM	Ver propostas Técnica e Comercial
	Instalada na configuração máxima do equipamento	Conforme Edital	N/A	SIM	Anexo 19K (todas as páginas)
	Hot-Swappable / Hot-Pluggable	Conforme Edital	N/A	SIM	Anexo 17
5 - Fonte de Alimentação	Deverá possuir alimentação elétrica de acordo com a localidade onde serão instalados os equipamentos, na frequência de 60Hz	Conforme Edital	N/A	SIM	Anexo 19K (todas as páginas)
	Fontes redundantes internas e independentes com alimentação redundante	Conforme Edital	N/A	SIM	Anexo 19K (todas as páginas) Anexo 17 - pág. 12

CISCO SYSTEMS

Cisco 3700 Series **Multiservice** Access Routers

Access Platform Optimized for the Modular Integration of Branch Office Applications and Services

Introduction

The Cisco® 3700 Series Multiservice Access Routers are a family of modular routers tha enable flexible and scalable deployment of new e-business applications for the Full Servi branch office. The Cisco 3700 Series routers optimize the branch office with high perform routing, integrated low density switching, Security, Voice, IP telephony, Video and Cont Networking in a single integrated solution. This unique integrated design enables enterp customers to incrementally adapt to evolving business needs by enabling important serv delivered by Cisco IOS®, such as Quality of Service (QoS), IP Multicast, VPN, Firewall, Intrusion Detection, with the performance required for tomorrows business challenges. Cisco 3700 Multiservice Access Routers are based on the same modular concepts as the C 3600 Series but enable dramatically higher levels of performance and service integratior the branch office.

Figure 1 The Cisco 3700 Series Multiservice Access Routers

The Cisco 3725 and Cisco 3745 provide on-board LAN/WAN connectivity, new high-de service modules (HDSM), and support for multiple Advanced Integration modules (AIM deliver the highest levels of service density for the enterprise branch office today. Improvi the success of the Cisco 3600 Series' modular architecture, these highly integrated platfo deliver a compelling value proposition with by integrating components previously purch separately, such as two fixed 10/100 LAN ports and additional memory. With the optior two or four network module slots—which can be adjusted to accept the HDSM modules—three WAN Interface Card (WIC) slots, and two on-board AIM slots, the Cisco offers many flexible options to enable high densities of services. Providing support for th majority of LAN and WAN interfaces available today on the Cisco 3600 Series platform reinforces Cisco investment protection promise and maximizes the flexibility of these plati for the future.

Cisco 3700 Multiservice Access Router Overview

The modular Cisco 3700 Series Multiservice Access Routers leverage network modules (NMs), WAN Interface Cards (WICs), and Advanced Integration Modules (AIMs) from the Cisco 1700, 2600, and 3600 Series Routers for WAN Access, Voice Gateway, Security, Content, and Dial applications. In addition, the Cisco 3725 and Cisco 3745 introduce a new, doublewide form factor, that provides support for the high density services modules (HDSM's). The Cisco 3745 with four network module slots can accept up to two HDSM's by removing the center guides between each pair of adjacent NM slots. The Cisco 3725, with two network module slots can accept a single HDSM in the upper network module slot by removing the blank panel and still have an available network module slot. By utilizing the new HDSM capability the Cisco 3700 Series routers are able to integrate higher port density and new, high performance services.

Figure 2 Cisco 3745 Multiservice Access Router (shown with optional interfaces)

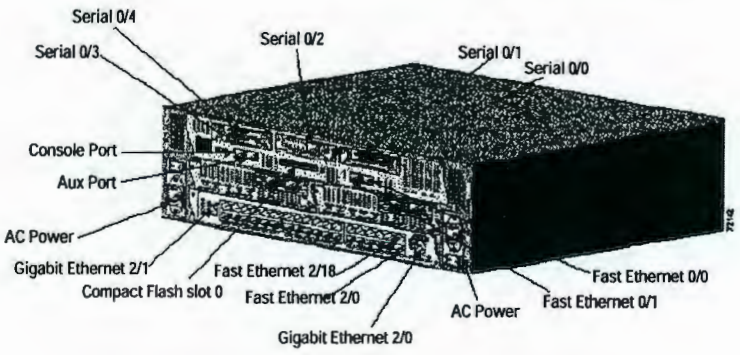
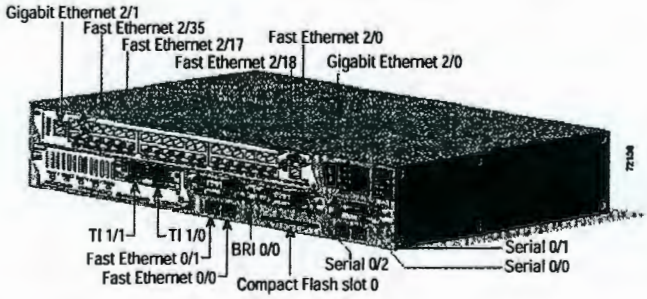


Figure 3 Cisco 3725 Multiservice Access Router (shown with optional interfaces)



Also new in the Cisco 3700 Series is the ability to support integrated In-Line Power on optional 10/100 switching modules for IP Telephony and/or Aironet Wireless LAN applications. By integrating the connectivity slots and ports on the base chassis, the Cisco 3700 Series enables the NM slots to integrate additional services in a small footprint. Both Cisco 3700 platforms offer increased Flash and DRAM default memory to accelerate and simplify future service and feature additions. In addition, the Cisco 3745 router offers additional availability features that may be required in high density, multiple services configurations.

Key features for the Cisco 3725 and 3745:

- Two Integrated 10/100 LAN ports
- Two Integrated Advanced Integration Modules (AIM) slots
- Three Integrated WAN Interface Card (WIC) slots
- Two (Cisco 3725) or four (Cisco 3745) Network Module (NM) slots
- One (Cisco 3725) or two (Cisco 3745) High Density Service Module (HDSM)-capable slots
- 32MB Compact Flash/ 128MB DRAM (default, single 128MB DIMM/SODIMM)
- Both Cisco 3725 and 3745 have a single 128MB SDRAM DIMM module and a single 32MB Compact Flash module by default
- Optional In-Line Power for 16-port EtherSwitch NM, 36-port EtherSwitch HDSM and wireless access points
- Support for all major WAN protocols and media: LL, FR, ISDN, X.25, ATM, fractional T1/E1, T1/E1, xDSL, T3/E3, HSSI
- Support for selected NMs, WICs and AIMs from the Cisco 1700, 2600 and 3600 Series
- 2 RU (Cisco 3725) or 3 RU (Cisco 3745) Rack-mountable chassis
- -24V DC power supply
- NEBS Level 3 compliance

Additional Key Features for the Cisco 3745:

- Field-replaceable motherboard, I/O board and fan tray
- Passive backplane
- Optional internal redundant power supplies (RPS — AC, DC and inline power)
- Online Insertion and Removal (OIR) of NMs and RPSs

Table 1 Cisco 3700 Series Key Features and Benefits

Feature	Benefit
Investment Protection	
Modular platform which shares interfaces with Cisco 1700, 2600, 3600	• Network interfaces are field-upgradable to accommodate future technologies – Additional services can be added on an "integrate as you grow" basis – Leverages the large existing portfolio of WICs, VICs, NMs and AIMs to reduce sparing, training, configuration and installation and maintenance costs
LAN/WAN Connectivity integrated into chassis	• More NM and HDSM slots available to add services in the future – Combination of AIMs and WICs along with NMs/HDSMs gives greater flexibility to create new configurations as requirements change
VPN and Security configurations	• Add security intrusion detection (IDS) and VPN connectivity to the router through Cisco IOS software and optional performance-enhancing data encryption AIMs. – Provides secure connectivity and perimeter security throughout the network.
Flexible voice gateway and IP Telephony configurations	• Incremental or full scale migration from legacy infrastructure to IP Telephony – Supports numerous standards-based analog and digital interfaces to PBXs and the PSTN – Sliding scale options for higher density mixed analog and digital voice gateway configurations

Table 1 Cisco 3700 Series Key Features and Benefits (Continued)

Feature	Benefit
Cisco IOS software	• Supports Cisco IOS feature sets common with the Cisco 2600 and 3600 routers – Enables end to end solutions with full support for Cisco IOS-based QoS, bandwidth management and Security mechanisms
Scalability	
Increased AIM (2) and WIC density (3)	• Services and WAN connectivity and backup can be supported without consuming an NM slot – Increased density per RU of voice, switching, WAN connectivity
Increased default memory of 32MB Compact Flash and 128MB DRAM	• A greater number of new Cisco IOS releases may be added without the need to purchase/install additional memory
New High Density Service Modules (HDSM)	• Enables higher port density and new, high performance services
Availability	
Support for Optional Redundant Power	• Accommodates optional RPS (external for Cisco 3725, internal for Cisco 3745) and minimizes network downtime
Survivable Remote Site Telephony	• Branch offices can leverage centralized call control while cost-effectively providing local branch backup redundancy for IP Telephony
Online Insertion and Removal-capable (3745 only)	• Allows network modules to be swapped or serviced with minimal impact to network availability – Allows servicing of online replacement of RPS – Online replacement of fan tray
Field-replaceable motherboard, I/O board, power supplies and fan tray (3745 only)	• High serviceability design – Additional operations and maintenance flexibility

Advanced Integration Module Options

The Cisco 3700 Series are equipped with two internal slots to support one or two field-installable AIMs. AIMs use function-specific hardware to off-load the main router CPU and accelerate processor- or resource-intensive services, yielding dramatically higher throughput and higher performance than a software-only implementation. The AIM slot has access to virtually all of the router's resources, including the main system bus. The TDM bus and the serial communications controllers make this a very flexible and powerful feature. Since the AIM is internally mounted, external slots remain available for integration of other modular components such as CSU/DSUs, WAN interfaces, or other devices such as modems, or packetized voice/fax processors.

The Data Compression AIM provides a cost-effective option for reducing recurring WAN costs and maximizes the benefit of the advanced bandwidth management features of the Cisco IOS software. With compression ratios of up to 4:1, each integrated Data Compression AIM supports 4 T1/E1s of compressed data throughput with one AIM and up to 8 T1/E1 with two AIMs. The Data Compression AIM supports industry standard LZS and Microsoft Point-to-Point Compression (MPPC) algorithms and ensures compatibility with all Cisco products supporting hardware- or software-based compression.

Three combination Voice + ATM AIM modules are available on the Cisco 3700 Series. The AIM-ATM provides asynchronous transfer mode (ATM) services to the WAN. The AIM-VOICE-30 provides digital signal processor (DSP) services, which can support up to 30 medium-complexity voice channels. The AIM-ATM-VOICE-30 combines the features from the AIM-ATM and AIM-VOICE-30 modules onto a single AIM module. These AIM modules supplement the broad portfolio of Cisco voice solutions and allow enterprises and service providers the flexibility of implementing ATM and voice solutions on the routers. These three Voice and ATM AIM modules provide a cost-effective option for reducing recurring cost and maximizing the benefits of the advanced bandwidth management features of the Cisco IOS software.

The AIM-ATM offers ATM adaptation layer 2 (AAL2) and ATM adaptation layer 5 (AAL5) support for low-density T1/E1 data and voice connections over ATM networks. It supports the following ATM-IMA capabilities: up to 4 T1/E1 of IMA with a single AIM-ATM, and 8 T1/E1 of IMA with two AIM-ATM's (maximum 4 T1/E1 IMA bundle). This AIM module allows service providers and enterprise customers to take advantage of the reliability and quality of service (QoS) available with ATM connectivity. The AIM-VOICE-30 contains DSPs that can support up to 30 medium-complexity voice channels when used with the Voice/WAN (VWIC-MFT) interface card. When the AIM-VOICE-30 can be used in a Cisco 3700, for voice over IP (VoIP) or voice over Frame Relay (VoFR) connectivity while freeing up the network module slot for other applications. The AIM-ATM-VOICE-30 combines the ATM features of AIM-ATM and voice features of AIM-VOICE-30 in a single AIM

4-Gerd?

The Data Encryption AIM's available for the Cisco 3700 Series offloads encryption processing from the CPU, providing over 10 times the performance over software-only encryption. The AIM-VPN/EP on the Cisco 3725 supports a maximum of 800 tunnels. On the Cisco 3745, the AIM-VPN/HP supports a maximum of 1,800 tunnels. The recently released AIM-VPN/EPII and AIM-VPN/HPII further extends the encryption performance of the Cisco 3700. These modules offers hardware accelerated DES/3DES and the new AES (Advanced Encryption standard) encryption at speeds up to 90-Mbps on the Cisco 3745 (max based on 1400 byte packet size). In addition the AIM-VPN/EPII and AIM-VPN/HPII support hardware-assisted layer-3 compression services where bandwidth conservation may lower network connection costs. The AIM-VPN/EPII on the Cisco 3725 supports a maximum of 8,000 tunnels, and the Cisco 3745, with the AIM-VPN/HPII supports a maximum of 10,000 tunnels.

Key Applications and Benefits

The Cisco 3700 platforms are designed for the Full Service Branch office that are deploying advanced applications, that require higher performance for voice, security, QoS, content acceleration and delivery, and high availability at the network edge by integrating functions previously addressed by a combination of platforms.

Advanced Security Services and VPN's

The Security and VPN features of the Cisco 3700 offer customers the ability to deploy proven security features such as secure VPNs, Intrusion Detection Systems (IDS), and firewalls, as well as high-speed Internet access and the ability to create extranets or demilitarized zones (DMZs). Cisco access routers deliver a rich, integrated package of routing, firewall, intrusion detection, and VPN functions for multiservice applications.

VPNs help companies reap benefits such as dramatically lowered WAN costs, improved global connectivity, and better reliability, while enabling capabilities such as secure extranet communications. Remote dial, Internet, intranet, and extranet access can all be consolidated over a single WAN connection to the Internet. The Cisco 3700 VPN solution supports the features essential to VPNs—IPSec data encryption, tunneling, broad certificate authority support for

public key infrastructure (PKI)—and advanced features such as stateful VPN failover, certificate auto-enrollment, stateful firewall, intrusion detection, and service-level validation. The Cisco 3700 Series works with optional Virtual Private Network Modules (VPN Modules) to optimize the platforms for virtual private networks (VPNs). The Cisco 3700 Series VPN Modules provide up to 10 times the performance over software-only encryption by offloading the encryption processing from the router central processing unit (CPU). The Cisco 3700 series together with the VPN module are the perfect IPSec VPN solution for connecting medium, and large branch offices to other remote locations, corporate headquarters, central-office intranets, or partner extranets.

As network security becomes increasingly critical to securing business transactions, businesses must integrate security into the network design and infrastructure. The Cisco IOS Firewall is a security-specific option for Cisco IOS software which runs on the Cisco 3700 platform. It integrates robust firewall functionality and intrusion detection for every network perimeter and enriches existing Cisco IOS security capabilities. It adds greater depth and flexibility to existing Cisco IOS security solutions—such as authentication, encryption, and failover—by delivering state-of-the-art security features such as stateful, application-based filtering; dynamic per-user authentication and authorization; defense against network attacks; Java blocking; and real-time alerts.

VPN Security Features and Voice and Video-Enabled IPSec VPN

The Cisco 3700 VPN security features are all voice and video-enabled IPSec VPN ready. The Cisco 3700 offers a VPN infrastructure capable of transporting converged voice, video, and data traffic across a secure IPSec network. The Cisco 3700 VPN platforms are able to accommodate the diverse network topologies and traffic types characteristic of multiservice IPSec VPNs, and ensure that the VPN infrastructure does not break multiservice applications deployed now or in the future.

The network architecture of the Cisco Voice and Video-Enabled IPSec VPN (V3PN) Solution takes advantage of Cisco VPN routers with Cisco IOS Software, Cisco CallManager, and IP phones. Furthermore, Cisco provides an overall deployment model for these products through Cisco AVVID (Architecture for Voice, Video and Integrated Data) for converged networking and the SAFE Blueprint for VPNs. These deployment models ensure a secure, interoperable, reliable network solution with end-to-end product support.

Content Acceleration and Delivery

Cisco 3700 Series enables key services critical to supporting the needs of today's enterprise networks. By enabling efficient delivery of rich media and web content, content acceleration and delivery services enhance user productivity while optimizing WAN bandwidth. Cisco 3700 supports the integrated Content Engine Network Module, which leverages the advanced content acceleration features of the Cisco Content Engine 5xx Series into the industry's first router-integrated content delivery system.

As enterprises learn to capitalize on the capabilities of web-based applications, HTTP traffic is assuming a larger proportion of WAN bandwidth. The Content Engine Network Module effectively accelerates applications by optimizing the delivery of bandwidth-intensive and frequently accessed content. Caching alone can offer a 40-60% savings in WAN bandwidth usage by a branch site, and the content delivery capabilities of the module enables enterprise services which maximize the productivity and efficiency of a global enterprise. Integration of the application layer services of the Content Engine Network Module with intelligent network services such as QoS, compression and IPSec offer a superior bandwidth optimization solution for the enterprise branch.

Combining intelligent caching, content filtering and content delivery capabilities with robust branch office routing helps users optimize their networks for important branch IP services such as VOIP, while greatly simplifying configuration, deployment, and operation of network services. Running Cisco Application and Content Networking System (ACNS) software, the Content Engine Network Module enables customers to extend the value of their branch router infrastructure to deliver strategic new application services – such as Employee Internet Management, Streaming Media, live and on-demand e-communications and e-learning, with no performance degradation of core routing services. Further, the Content Engine Network Module interoperates with all Cisco devices, and leverages key Cisco IOS features such as multicast and WCCP while supporting key management solutions such as CiscoWorks.

Integration of Flexible Routing and Low Density Switching

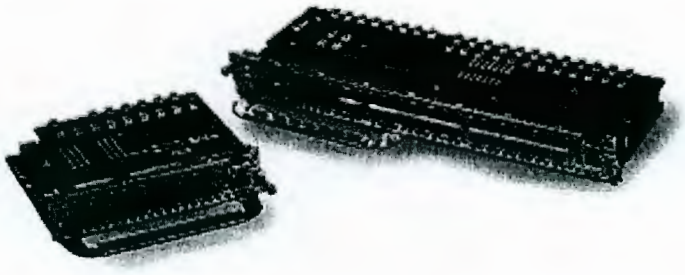
The Cisco 3700 Series offers an optional 16-port 10/100 EtherSwitch network module (NM), or an optional 36-port 10/100 EtherSwitch high density service module (HDSM), both of which leverage the proven Cisco Catalyst technology. The EtherSwitch NM/HDSM hardware supports 802.1p Layer 2 prioritization, while Cisco IOS supports Layer 3 Diff-Serv and Class of Service (CoS) markings for critical business data. Coupling Layer 2/3 prioritization techniques, with the QoS for the WAN, the Cisco 3700 Series ensures low latency for critical business applications, enabling the deployment of e-business applications.

The EtherSwitch ports can also be used to power the Cisco Aironet Access Points in the low-density-branch to deliver Wireless LAN (802.11b) access flexibility. The Cisco 3700 Series with the EtherSwitch NM/HDSM integrates Cisco IOS routing and Catalyst switching technologies in a single platform, offering a single point of management for easier configuration, troubleshooting and a lower total cost of ownership.

Key features include:

- Combination of the industry-leading Cisco IOS features with Catalyst switching technologies for wire-rate Layer 2 switching, with rich protocol and feature support.
- Integrated platform, with EtherSwitch ports for LAN, WAN flexibility, and a rich QoS toolkit for e-business applications.
- Enables simple, single point for configuration and troubleshooting, while integrating diverse technologies.
- Modular design enables scaling as business needs evolve with options for 16- or 36-port EtherSwitch module port densities.

Figure 4 Cisco 16- and 36-port EtherSwitch Modules



Single Platform Solution for Branch Office IP Telephony and Voice Gateway

As the migration to converged voice/data networks accelerates, enterprises need to deploy a platform that has the ability to immediately or gradually grow to support a wide range of traditional telephony devices in addition to newer IP telephony solutions. The Cisco 3700 Series delivers on that need by supporting legacy phone systems through a variety of scalable analog telephony connectivity options starting at two analog ports and scaling to 16, 32, 48 or 64 analog ports. Digital telephony connectivity is just as scalable with options beginning at 12 channels and scaling up to up to 240 channels. IP telephony solutions are also supported on the Cisco 3700 Series through a powerful set of features including line powered IP phone connectivity that begins with 16 ports and scales to 36, 52, or 72 ports in a single platform.

The performance-tuning of the Cisco 3700 Series enables customers to apply quality of service, bandwidth optimization and fragmentation services, along with other advanced call admission control, call control and queuing mechanisms, without sacrificing the expected data performance needed for future growth. The Cisco 3700 Series offers resilient IP telephony services, including Survivable Remote Site Telephony (SRST), H.323, SIP and MGCP, and redundant power for the system and IP phones.

With the Cisco 3700 Series, enterprises can deploy this scalable platform to support all of their telephony needs without investing in all connectivity requirements in the initial deployment. The enhanced service density of the Cisco 3700 allows enterprises the opportunity to deploy a base level configuration that will scale to the converged telephony needs of that branch when necessary. This modular telephony format mitigates future technology lockout.

Deployment of IP Telephony infrastructure solutions are facilitated by the following key Cisco 3700 features:

- Optional modular integration of an inline-powered EtherSwitch NM or HDSM, combined with analog and/or digital high-density voice gateway modules and flexible WAN connectivity for a modular, single-platform IP Telephony infrastructure
- Resilient IP Telephony services, including Survivable Remote Site Telephony (SRST), H.323, SIP and MGCP, and redundant power for system and IP phones
- Complete Cisco CallManager support for both H.323 and MGCP call control protocols makes the Cisco 3700 the ideal voice gateway
- Performance-tuned to scale both analog, and digital voice solutions and hybrid solutions
- Modular expandability enables the addition of gateway or phone aggregation ports as needed
- Integrated Time Division Multiplexing (TDM) for full Drop&Insert functionality between all WIC, Network Module and onboard AIM's

The evolution from traditional TDM voice to IP Telephony has created the requirement that branch offices be equipped to deploy IP Telephony solutions without the need to replace the branch office access platforms. The Cisco 3700 series fulfills that need by ensuring complete support for the range of voice gateway densities and IP Telephony features necessary for Enterprises' evolving branch office infrastructures.

Figure 5 Cisco 3700 Full Serivce Branch integrated capabilities

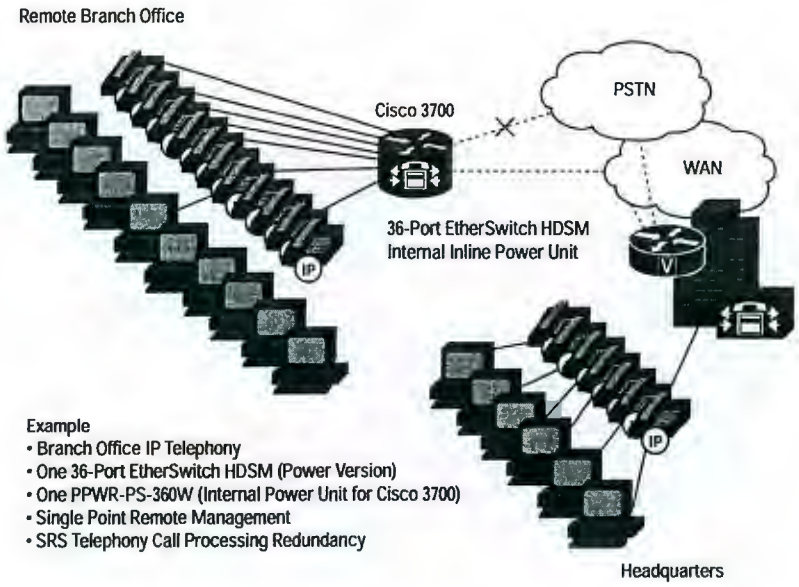
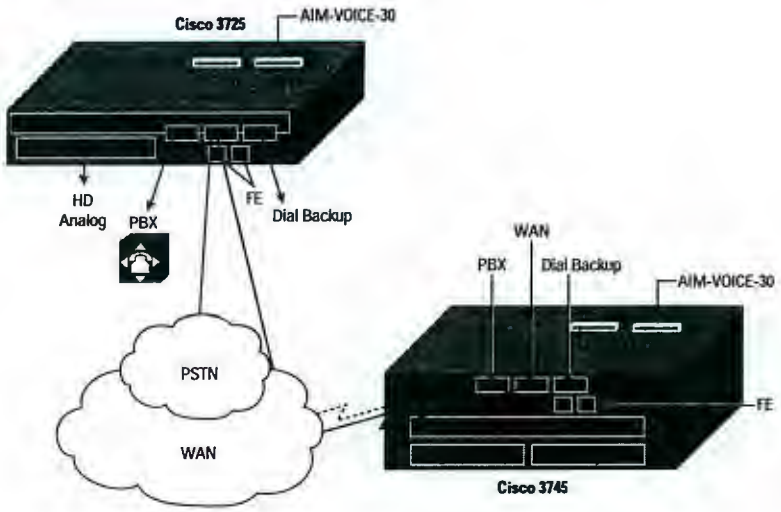


Figure 6 Full Service Branch scenarios



Cisco 3700 enables higher service densities through a versatile, wider interface form factor (using a HDSM), additional interface options with three WIC slots, CPU offload with two built-in AIM slots, and on-board LAN/WAN connectivity to free up module slots.

Table 2 Supported Interfaces for the Cisco 3700 Series

Interfaces	Description
LAN/WAN	• FE Combo NMs (NM-1FE2W, etc.) • 1 port Multimode Fiber FE NM • 1 port Gigabit Ethernet GBIC NM • 1 port ADSL WIC • 1 port G.SHDSL WIC
LAN	• 16 & 36 port EtherSwitch NMs
Serial	• 2 port Serial WIC • 1 and 2 port T1/E1 CSU/ DSU VWICs • 1 port 56k CSU/DSU WIC • 4 and 8 port Sync/Async Serial NMs • HSSI NM1 port T1 CSU/DSU WIC • 16 & 32 port Async NMs • 1 port serial WIC • 4 port serial NM • 1-port T3/E3 with Integrated DSU
ISDN/Channel	• 1 and 2 port T1/E1 Channelized/ ISDN Pri NMs • 4 and 8 port T1/E1 ISDN BRI NMsISDN BRI WICs
Voice	• Low Density Analog Voice NMs (all VICs except BRI NT/TE) • High Density Analog Voice NM • High density T1/ E1 Digital Voice NMs • BRI NT/TE VIC • DSP AIM
ATM	• 4 and 8 port T1/E1 NMs • 1 port DS3 / E3 NMs • SAR AIM • SAR/DSP AIM
Modem	• Digital Modem NMs • 1 and 2 port Analog Modem WICs • 4 and 8 port Analog Modem NMs
Services	
Security, VPN and Compression	• EP & HP Encryption AIMs • EP & HP II Encryption AIMs • COMPR4 AIM • Layer 2 Data Compression • Intrusion Detection NM
Content Delivery	• Content Engine NM

Specifications

Table 3 Cisco 3700 Series Specifications

Description	Specification
Processor Type	• Cisco 3725—MIPS RISC processor • Cisco 3745—MIPS RISC processor
Performance	• Cisco 3725—100kpps • Cisco 3745—225kpps
Flash Memory (Compact Flash)	• Internal: 32MB (default), expandable to 128MB • External: 32MB, 64MB,128MB options
System Memory	• 128MB (SDRAM default)—expandable to 256MB
Integrated WIC slots	• 3
Onboard AIM (internal)	• 2
Console port	• 1 (up to 115.2 kbps)
Aux port	• 1 (up to 115.2kbps)
Minimum Cisco IOS Release	• Cisco IOS 12.2(8) T
Onboard LAN ports	• 2 10/100 Fast Ethernet ports
Redundant Power Supply Support	• Cisco 3725—Universal DC (24VDC to 60VDC), PWR600-AC-RPS External RPS • Cisco 3745—Internal Redundant options for AC and Universal DC (24VDC to 60VDC)
Rack Mounting	• Yes, 19' and 23" options
Power requirements	
Power Supply	• Cisco 3725— – 135W Maximum AC to DC power supply – 495W Maximum with optional power supply:,-48V@360W) AC to DC power supply • Cisco 3745— – 230W Maximum ()AC-DC Power Supply – 590W Maximum (Per AC Input) with optional power supply -48V@360W) AC-DC power
Heat Dissipation	• Cisco 3725— – 135W Maximum 460.661 BTU/hour – 495W Maximum 1689.089 BTU/hour • Cisco 3745— – 230W Maximum 784.829 BTU/hour – 590W Maximum 2013.257 BTU/hour
Output	• Cisco 3725— – (optional -48V@7.5A) • Cisco 3745— – (optional -48V@7.5A)

Table 3 Cisco 3700 Series Specifications (Continued)

Description	Specification
AC input voltage	• 100 to 240VAC
Frequency	• 47-63Hz
AC input current	• Cisco 3725— – 2A max @ 100VAC;1A max @ 240VAC (215W Maximum) with optional power supply: – 7A Max@100VAC;3.5A max @ 240VAC (665W Maximum) • Cisco 3745— – 5A max @ 100VAC;2.5A max @ 200VAC (365W Maximum) with optional power supply: – 10A max @100VAC;5A max@200VAC (815W Maximum)
Environmental Specifications	
Operating temperature	• 32 to 104 F (0 to 40 C)
Nonoperating temperature	• -40 to 185 F (-40 to 85 C)
Relative humidity	• 5-95% noncondensing
Operation altitude	• Up to 6500 ft (2000m), derate 1C per 1,000 ft.
Dimensions (HxWxD)	• Cisco 3725—3.5 x 17.1 x 14.7 in. • Cisco 3745—5.25 x 17.25 x 16 in.
Weight (without NMs or WICs or additional Power Supplies)	• Cisco 3725—14 lbs. • Cisco 3745—32 lbs.
Regulatory Compliance	
Safety	• UL 1950 • CAN/CSA-C22.2 No. 950 • EN 60950 • IEC 60950 • TS 001
EMC	• FCC Part 15 • ICES-003 Class A • EN55022 Class A • CISPR22 Class A • AS/NZS 3548 Class A • VCCI Class A

Table 3 Cisco 3700 Series Specifications (Continued)

Description	Specification
Telecom	• FCC Part 68 • Canada CS-03 • JATE • RTTE Directive
Interface Support	
High Density Service Modules	NMD-36-ESW, NMD-36-ESW-2GIG, NMD-36-ESW-PWR, NMD-36-ESW-PWR-2G
Network Modules	NM-16ESW, NM-16ESW-PWR, NM-16ESW-1GIG, NM-16ESW-PWR-1GIG, NMD-36-ESW, NMD-36-ESW-PWR, NMD-36-ESW-2GIG, NMD-36-ESW-2G, NM-1FE-FX-V2, NM-1FE2W, NM-2FE2W, NM-1FE1R2W, NM-2W, NM-1HSSI, NM-4A/S, NM-4B-S/T, NM-4B-U, NM-8A/S, NM-8B-S/T, NM-8B-U, NM-1CT1, NM-1CT1-CSU, NM-2CT1, NM-2CT1-CSU, NM-1CE1B, NM-1CE1U, NM-2CE1U, NM-2CE1B, NM-4E1-IMA, NM-4T1-IMA, NM-8E1-IMA, NM-8T1-IMA, NM-1A-T3, NM-1A-E3, NM-1V, NM-2V, NM-HDA-4FXS, NM-HDV-1T1-12, NM-HDV-1E1-12, NM-HDV-1E1-30, NM-HDV-1E1-30E, NM-HDV-2E1-60, NM-HDV-1T1-24, NM-HDV-2T1-48, NM-HDV-1T1-24E, NM-HDV-2T1-48, NM-6DM, NM-12DM, NM-18DM, NM-24DM, NM-30DM, NM-16A, NM-32A, NM-1A-OC3MM, NM-1A-OC3SMI, NM-1A-OC3SML, NM-1A-OC3MM-EP, NM-1A-OC3SMI-EP, NM-1A-OC3SML-EP, NM-1GE, NM-1T3/E3, NM-CE-BP-SCSI-K9, NM-CE-BP-20G-K9, NM-CE-BP-40G-K9, NM-4T, NM-8AM, NM-16AM
WICs, VWICs, and VICs	WIC-2T, WIC-2A/S, WIC-1B-S/T, WIC-1B-U, WIC-1DSU-56K4, 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, WIC-1ADSL, WIC-1AM, WIC-2AM, VIC-2DID, VIC-2FXS, VIC-2FXO, VIC-2FXO-EU, VIC-2FXO-M1, VIC-2FXO-M2, VIC-2FXO-M3, VIC-2E/M, VIC-2CAMA, VIC-2BRI-S/T-TE, WIC-1T, WIC-1DSU-T1, WIC-1SHDSL, VIC-2BRI-NT/TE
AIMs	AIM-VPN-HP, AIM-VPN-EP, AIM-VPN/EPII, AIM-VPN/HPII, AIM-ATM, AIM-VOICE-30, AIM-ATM-VOICE-30, AIM-COMPR4

Ordering Information

The Cisco 3700 Series is orderable through the following part numbers:

Part Number	Description
CISCO3725	3700 Series, 2-Slot, Dual FE, Multiservice Access Router
CISCO3745	3700 Series, 4-Slot, Dual FE, Multiservice Access Router

Summary

The Cisco 3700 Series Multiservice Access Routers enable flexible and scalable deployment of new e-business 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 edge for Branch Office IP Telephony, voice gateway, and integrated flexible routing with low-density switching solutions. In addition, the Cisco 3700 Series provides a consolidated service infrastructure and high service density in a compact form factor that enables the incremental integration of branch applications and services.

Service and Support

The award-winning Cisco Service and Support offerings provide presales network audit planning, design consulting, network implementation, operational support, and network optimization. By including service and support when purchasing Cisco 3700 products, customers can confidently deploy a converged network architecture using Cisco expertise, experience, and resources.

For More Information on Cisco Products, Contact:

U.S. and Canada: 800 553-NETS (6387)

Europe: 32 2 778 4242

Australia: 612 9935 4107

Other: 408 526-7209

Web: 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

ANEXO 17A

23975 Paula

Data Sheet

Cisco T3/E3 Network Module for Cisco 2600, 3600, and 3700 Series Routers

The Cisco T3/E3 Network Module provides high-speed WAN access for the Cisco 2600, 3600, and 3700 series routers. T3/E3 WAN access enables the network to carry high volumes of data and rich multimedia content, while providing low latency for voice over IP (VoIP).

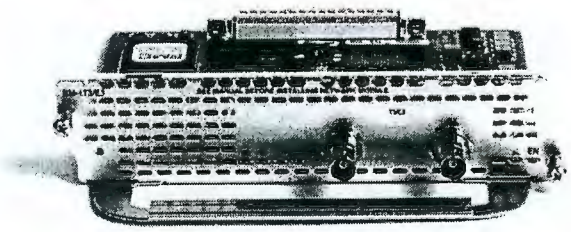
Cisco's Packet-over-T3/E3 network module for the Cisco 2600, 3600, and 3700 series offers the first software-configurable T3/E3 product from Cisco. This flexible network module allows the customer to switch between T3 and E3 applications with a single Cisco IOS® command. This feature provides customers with unparalleled investment protection by allowing the service provider or enterprise customer to stock only a single product that can be deployed internationally.

The demand for increased bandwidth has led to growth in clear-channel T3/E3 deployment. This new Packet-over T3/E3 network module (part number NM-1T3/E3) eliminates the need for an external data service unit (DSU), reduces provisioning costs, and provides highly manageable T3/E3 line termination. The module provides an integrated line interface unit (LIU) DSU that allows T3 or E3 lines to be directly terminated on a Cisco router, eliminating the need for external DSU equipment. This simplifies the T3/E3 line management, reduces provisioning cost, and frees valuable rack space.

Offering unprecedented flexibility in provisioning clear-channel T3 or E3 connections, the Cisco T3/E3 network modules provide support for the proprietary subrate and scrambling features of T3 DSU vendors Digital Link, Larscom, and ADC Kentrox. Subrate support in the Cisco T3/E3 Network Module maximizes the utility of these products in service provider environments for tiered DS3 services. By simultaneously supporting interoperability with a wide range of third-party DSU vendors, this network module offers the flexibility to support installed equipment without locking customers into a proprietary solution.

The Cisco T3/E3 Network Module provides direct connectivity to a T3 line for full-duplex communications at the T3 rate of 44.736 MHz and full-duplex E3 communications at 34.368 MHz. Each T3 or E3 port consists of a pair of 75-ohm BNC coaxial connectors (Type RG-59), one for transmit data and one for

Figure 1
Cisco T3/E3 Network Module



receive data, along with six LED indicators for line status. The Cisco 2650XM and 51XM, Cisco 2691, Cisco 3660, and the Cisco 3725 support a single T3/E3 network module. The Cisco 3745 supports up to two single-port Cisco T3/E3 network modules.

Because the Cisco T3/E3 Network Module is supported in Cisco IOS feature sets, including IP Only, there are no additional memory requirements for any supported platforms.

Key Benefits

The combination of T3 and E3 options in a single network module provides numerous important customer benefits:

- Physical space savings—Eliminates the need for external DSU device, saving valuable rack space
- Simplified management—Eliminates the need for two separate monitoring tools
- Software-configurable T3/E3—Provides the flexibility to deploy a single module worldwide

Key Features

- One-port T3 with DSU or E3 with DSU network module
- T3/E3-specific features for monitoring, bit error rate tester (BERT), Management Information Bases (MIBs), alarms, and more
- T3 configuration has the ability to independently or simultaneously enable scrambling and subrate in each DSU mode; support for the following DSU vendors' algorithms: Digital Link, Kentrox, Larscom, Verilink, Adtran
- E3 configuration has the ability to independently or simultaneously enable scrambling and subrate in the Kentrox DSU mode. Digital Link is also supported for subrate E3; but without a scrambling option per industry standard.
- Support for the serial encapsulation protocols: Frame Relay, Point-to-Point Protocol (PPP), High-Level Data Link Control (HDLC)
- 16-bit cyclic redundancy check (CRC)

Key Management Features

- Line and payload loopback capabilities
- DS3 remote-line loopback (via Far End Alarm and Control [FEAC] codes per American National Standards Institute [ANSI] T1.107a)
- Response to embedded loopback commands
- Insertion of loopback commands into transmitted signal
- Programmable pseudorandom pattern up to 32 bits long, including 223, 220, 215, 1s, 0s, alt-0-1
- 32-bit error count and bit-count registers
- Alarm detection—Alarm indication signal (AIS), remote alarm, far-end block error (FEBE), out of frame (OOF)
- Onboard processor for Maintenance Data Link (MDL)

T3/E3 Applications and Positioning

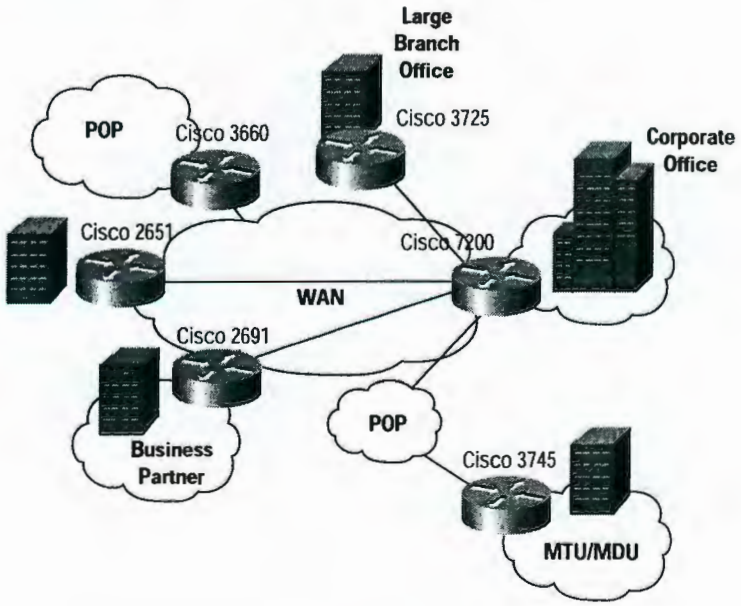
The Cisco T3/E3 Network Module provides the high-speed performance required to build today's advanced, fully converged networks that need to support a wide array of applications and services such as security, and advanced quality of service (QoS) for voice and video. T3/E3 and subrate T3/E3 connectivity allows customers to take the fullest advantage of their WAN

bandwidth for deploying the newest applications and service delivery. All the supported platforms are capable of supporting line-rate performance, but they use varying levels of CPU overhead and thus affect the overall platform performance. The Cisco 3745, for instance, is the highest-performing platform and is recommended for concurrent application environments where full wire rate is required. The Cisco 3725 and Cisco 3660 are the next highest-level performers; they have very similar CPU loading characteristics under comparable traffic conditions (refer to Table 1).

Table 1 Cisco T3/E3 Network Module Branch-Office Positioning

Supported Platform	Recommended Type of Service	Recommended Branch-office Size
Cisco 2650 and 2651XM	Subrate T3/E3	Small to medium office
Cisco 2691	Subrate T3/E3	Small to medium office
Cisco 3661 and 3662	Sub- and full-rate T3/E3	Large and regional office
Cisco 3725	Sub- and full-rate T3/E3	Medium and large office
Cisco 3745	Sub- and full-rate T3/E3 service	Medium, large, and regional offices

Figure 2
Typical Cisco T3/E3 Network Module Deployments



Specifications

Software Support

Table 2 lists the minimum Cisco IOS Software requirements for the Cisco T3/E3 Network Module, and Table 3 gives support information.

Table 2 Minimum Cisco IOS Software Requirements for Cisco T3/E3 Network Module

Product Number	Description	Minimum Cisco IOS Software Version
NM-1T3/E3	One-port clear-channel T3/E3 network module	12.2(11)YT

Table 3 MaximumT3/E3 Support Comparison

Supported Platforms	Maximum T3/E3 Supported
Cisco 2650 and 51XM	1
Cisco 2691	1
Cisco 3660	1
Cisco 3725	1
Cisco 3745	2

Hardware Specifications

DS3/E3 Specifications

- DSX3 level interface with dual female 75-ohm BNC coaxial connectors per port (separate RX and TX)
- Full- and half-duplex connectivity at DS3 rate (44.736 MHz)
- Full- and half-duplex connectivity at E3 rate (34.368 MHz)
- Scrambling and subrate support of major DSU vendors
- Line build-out—Programmable for up to 450 feet of 734A or equivalent coaxial cable or up to 225 feet for 728A or equivalent coaxial cable
- C-bit, or M23 framing for T3, bypass and G.751 framing for E3 (software selectable)
- Binary 3-zero substitution (B3ZS) (T3) or high-density bipolar with three zeros (HDB3) (E3) line coding
- Support for 16- and 32-bit CRC (16-bit default)
- DS3 FEAC channel support
- Twenty-four-hour history maintained for error statistics and failure counts
- DS3 alarm and event detection (once per second polling)
- Alarm indication signal (AIS)
- Out of frame (OOF)
- Line code violation (LCV)
- Excessive zeros (EXZ)
- Far-end receive failure (FERF)

Table 4 LED Port Indicators and Status

LED indicator	Color	Active state description
CD	Green	Carrier detect (off indicates loss of signal [LOS])
LP	Yellow	Loopback mode on
AIS	Yellow	Port is receiving AIS
FERF	Yellow	Port is receiving FERF signal
EN	Yellow	Network module is enabled
Alarm	Yellow	Port is receiving OOF errors

Serial Encapsulations

- HDLC
- PPP
- Frame Relay
- ATM Data Exchange Interface (ATM-DXI)

Physical Specifications

- Single-wide network module, no slot restrictions
- Dimensions (H x W x D) 1.55 x 7.10 x 7.2 inches (3.9 x 18.0 x 18.3 centimeters)

Environmental Specifications

- 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

Certification

Compliance

DS3 physical layer

- ANSI T1.102, T1.107

E3 physical layer

- TBR24
- ITU-T G.703 & G.823
- ACA TS016

Safety

- United States (UL1950 3rd Edition/CSA C22.2, No.950)
- Canada (C1950)
- UK (BS6301, EN60950, EN41003)
- Germany (TUV GS)
- France (EN60950, EN41003, NFC98020)
- AS/NZS 3260 (Australia/New Zealand)
- EN60950/EN41003 (Europe)
- IEC 950 (national deviations)

EMC

- 47 CFR 15: 2001 Class A (FCC)
- ICES003 Class A
- EN55022 Class A: 1998
- EN300386: 2001
- EN55024:1998, EN50082-1:1997 and EN61000-6-2: 1999 including:
  - ESD: EN61000-4-2
  - Radiated Immunity: EN61000-4-3
  - Burst Transients: EN61000-4-4
  - Surges: EN61000-4-5
  - Injected RF: EN61000-4-6
  - Dips + Sags: EN61000-4-11
- EN61000-3-2: 1995
- EN61000-3-3: 1995
- AS/NZS 3548 Class A
- VCCI V-3/2000.04 Class A

Standards

- T3/E3 MIB (RFC 1407)

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

2028831/ETMG 11/02

ANEXO 17B

Cisco Systems

Data Sheet

Cisco **Gigabit Ethernet Network Module**
for Cisco 2691, 3660, and 3700 Series Routers

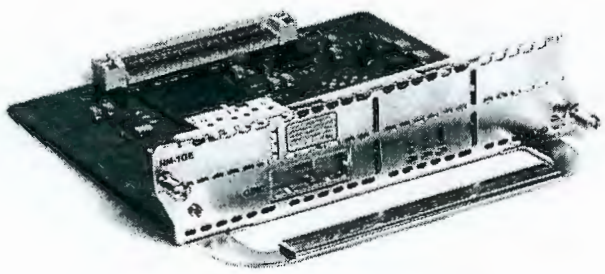
The Cisco Gigabit Ethernet Network Module brings Gigabit Ethernet to the Cisco 2691, 3660, and 3700 series routers to accelerate applications such as metropolitan (metro) access, inter-VLAN routing, and high-speed connectivity to LAN switches.

Overview

The single-port Cisco Gigabit Ethernet Network Module (part number NM-1GE) provides Gigabit Ethernet optical and copper connectivity for access routers. The module is supported by the Cisco 2691, Cisco 3660, Cisco 3725, and Cisco 3745 series routers. This network module has one gigabit interface converter (GBIC) slot to carry any standard copper or optical Cisco GBIC (see Table 1 for details). The flexibility to use different GBICs allows for making a choice depending on various factors, such as distance, cost, existing infrastructure, future expansion plans, and requirements.

The Cisco Gigabit Ethernet Network Module enables branch offices to cost-effectively utilize high-speed uplinks in a variety of environments (refer to Figure 1). The enhanced performance allows customers to enable new applications and services as well as providing greater capacity for existing inter-VLAN routing and bridging capabilities. Additionally, branch offices will now have the opportunity to connect to metropolitan-area networks (MANs). Cisco IOS® Software provides enhanced capabilities such as quality of service (QoS), network-based application recognition (NBAR), IP Security (IPSec), and Layer 3 virtual private networks (VPNs).

Figure 1
Cisco Gigabit Ethernet Network Module



Product Summary

Table 1 Cisco Gigabit Ethernet Network Module Product Numbers

Product number	Product description
NM-1GE	One-port Cisco Gigabit Ethernet Network Module
GBICs	
WS-G5483	Copper GBIC (1000BASE-T, Category 5 cabling, up to 100 meters)
WS-G5484	Short-wavelength GBIC (1000BASE-SX, up to 550 meters)
WS-G5486	Long-wavelength, long-haul GBIC (1000BASE-LX/LH, up to 10 km)
WS-G5487	Extended-distance GBIC (1000BASE-ZX, up to 100 km)
Coarse Wavelength Division Multiplexing (CWDM) GBICs	
CWDM-GBIC-1470	1000BASE-CWDM GBIC 1470 nm (gray)
CWDM-GBIC-1490	1000BASE-CWDM GBIC 1490 nm (violet)
CWDM-GBIC-1510	1000BASE-CWDM GBIC 1510 nm (blue)
CWDM-GBIC-1530	1000BASE-CWDM GBIC 1530 nm (green)
CWDM-GBIC-1550	1000BASE-CWDM GBIC 1550 nm (yellow)
CWDM-GBIC-1570	1000BASE-CWDM GBIC 1570 nm (orange)
CWDM-GBIC-1590	1000BASE-CWDM GBIC 1590 nm (red)
CWDM-GBIC-1610	1000BASE-CWDM GBIC 1610 nm (brown)

Note: WS-G5482= (1000BASE-T GBIC) is not supported.

Key Features

Ethernet and VLAN Features

- IEEE802.3 with IEEE802.2 Service Advertising Protocol (SAP)
- IEEE802.3 with IEEE802.2 and Subnetwork Access Protocol (SNAP)
- IEEE 802.1Q virtual LAN (VLAN) tagging
- Cisco Inter-Switch Link (ISL) support
- Flow control (802.3x)

Network Management-Related Features

- CiscoView
- Simple Network Management Protocol (SNMP) support
- Remote Monitoring (RMON) support
- Cisco's NetFlow accounting

QoS Features

- Weighted Random Early Detection
- Precedence setting and mapping (802.1p)
- Committed Access Rate (CAR)
- Access control list (ACL)
- Extended ACLs
- Voice and remaining QoS features, per platform and Cisco IOS Software version

Miscellaneous

- Jumbo frame support, up to 16 KB
- Cisco Group Management Protocol (GMP), Internet Group Management Protocol (IGMP) for multicasting
- Hot Standby Router Protocol (HSRP)
- Online insertion and removal (OIR)—network module OIR supported on Cisco 3660 and Cisco 3745
- Hot insertion and removal for GBICs on all platforms
- Media type or GBIC type display—`show interface` displays GBIC, media type

Gigabit Ethernet Applications

Gigabit Ethernet in the Branch Office

In a branch office, the Cisco Gigabit Ethernet Network Module can provide a high-speed uplink. Figure 2 shows the module being used to bridge non-routable protocols while simultaneously providing Layer 3 connectivity. The module is also useful in situations that require inter-VLAN routing with an ISL or IEEE 802.1q trunk, and in any LAN requiring fiber connectivity.

Figure 2
Gigabit Ethernet in LANs

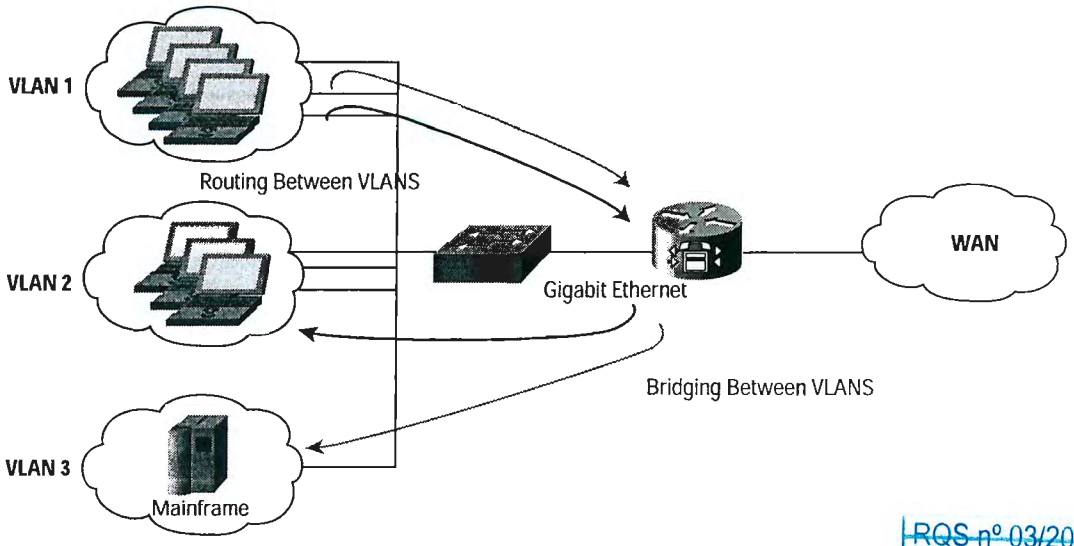
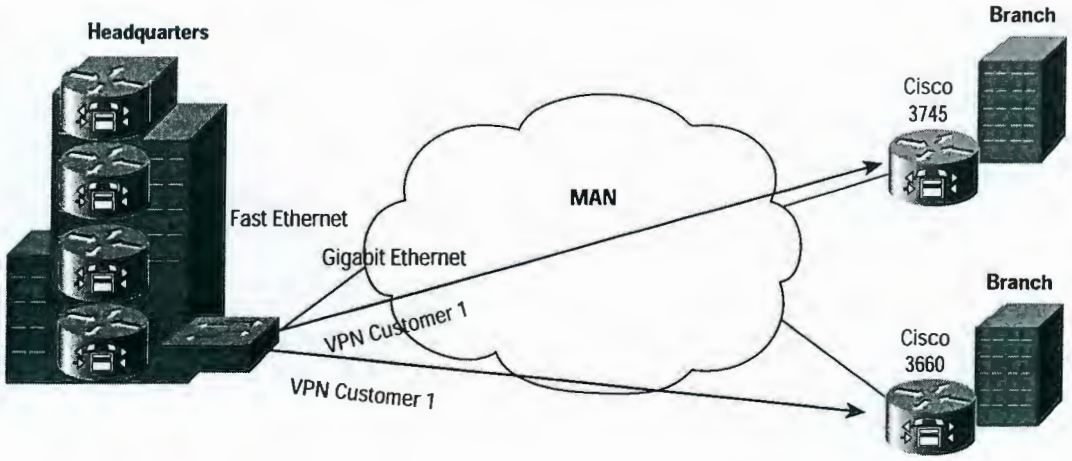


Figure 3 shows the Cisco Gigabit Ethernet Network Module being used to connect Layer 3 VPNs over a MAN. Cisco IOS Software enables QoS applications such as traffic shaping and NBAR. Again, this is ideal for situations in which fiber connectivity is desirable.

Figure 3
Gigabit Ethernet in MANs



Specifications

Software Support

Table 2 gives the Cisco IOS Software requirements for the Cisco Gigabit Ethernet Network Module, and Table 3 lists the platforms supported.

Table 2 Minimum Cisco IOS Software Requirements for Cisco Gigabit Ethernet Network Module

Product number	Minimum Cisco IOS Software version
NM-1GE	12.2(11)YT

Table 3 Maximum Cisco Gigabit Ethernet Network Module Support Comparison

Supported platforms	Maximum number of modules supported
Cisco 2691	1
Cisco 3660	2
Cisco 3725	1
Cisco 3745	2

Minimum Memory Requirements

Refer to the IOS Upgrade Planner or the Cisco IOS release notes for information regarding memory requirements.

Ethernet Specifications

- IEEE 802.3 with 802.2 SAP
- IEEE 802.3 with 802.2 and SNAP
- IEEE 802.1p
- IEEE 802.1q VLAN
- Cisco ISL
- Gigabit Ethernet IEEE 802.3z, IEEE 802.3x, IEEE 802.3ab

Agency Approvals

- UL 1950 (United States)
- CSA-C22.2 #950 (Canada)
- EN60950 (Europe)
- TUV GS (Germany)
- IEC 950 (International)

Electromagnetic Interference (EMI)

- FCC Part 15 Class A (United States)
- ICES-003 Class A (Canada)
- VCCI Class 2 (Japan)
- EN55022 Class B (Europe)
- CISPR 22 Class B (International)
- CE mark (Europe)

Physical Specifications

- Single-wide network module, no slot restrictions
- Dimensions (H x W x D) 1.55 x 7.10 x 7.2 inches (3.9 x 18.0 x 18.3 centimeters)

Environmental Specifications

- 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

Cisco 3745 and Gigabit Ethernet
A winning combination

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

202883/ETMG 11/02

ANEXO (18)

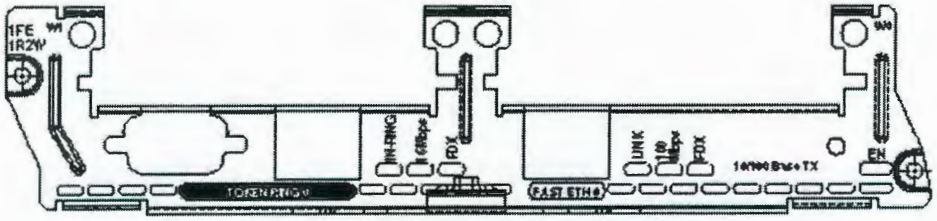
Understanding Fast Ethernet LAN/WAN Interface Card Netwo

Table of Contents

Understanding Fast Ethernet LAN/WAN Interface Card Network Modules

Introduction

The Fast Ethernet LAN/WAN interface card (WIC) Network Modules expand the capabilities of the Cisco 2600 and 3600 Series Routers, by providing slots for additional WICs. Some of these Network Modules also include Fast Ethernet or Token Ring ports for LAN connectivity.



Before You Begin

Conventions

For more information on document conventions, see the Cisco Technical Tips Conventions.

Prerequisites

There are no specific prerequisites for this document.

Components Used

This document is not restricted to specific software and hardware versions.

The information presented in this document was created from devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If you are working in a live network, ensure that you understand the potential impact of any command before using it.

Product Numbers

NM−1FE2W Network Module with One−Fast Ethernet and Two−WIC slots.

NM−1FE1R2W Network Module with One Fast Ethernet, One Token Ring and Two WIC slots.

NM−2FE2W Network Module with Two Fast Ethernet and Two WIC slots.

NM−2W Network Module with Two WIC slots and no LAN (Ethernet/Fast Ethernet) Ports.

See also the Ethernet LAN/WIC Network Modules.

Features

- **Fast Ethernet**
  - ♦ RJ−45 connector, 100 BaseT only.
  - ♦ Supports 10 and 100 Mbps, auto−sensing.
  - ♦ Supports full and half duplex.
  - ♦ Supports Inter−Switch Link (ISL) and Token Ring ISL in hardware (ISL requires the Cisco IOS® "Plus" feature set).
  - ♦ Does not support Fast EtherChannel.
  - ♦ Uses the same Fast Ethernet controller as all other Cisco 2600/3600 Fast Ethernet ports.
- **Token Ring**
  - ♦ RJ−45 and DB−9 connector (only one may be used at a time).
  - ♦ Supports full duplex Token Ring.
  - ♦ Uses the same Token Ring chip set as the Cisco 2612 and 2613.
- **WIC**
  - ♦ Supported WAN interface cards (WICs): WIC−1T, WIC−2T, WIC−2A/S, WIC−1B−S/T, WIC−1B−U, WIC−1DSU−56K4, WIC−1DSU−T1, WIC−1ADSL.
  - ♦ Supported Voice/WAN interface cards (VWICs): VWIC−1MFT−E1, VWIC−2MFT−E1, VWIC−2MFT−E1−DI, VWIC−1MFT−T1, VWIC−2MFT−T1, VWIC−2MFT−DI, VWIC−1MFT−G703, VWIC−2MFT−G703.
    - ◊ Supports a maximum of two channel groups per VWIC. Does not support ISDN PRI.
  - ♦ Not Supported: WIC36−1B−S/T, WIC36−1B−U, WIC−1B−S/T−LL, WIC−1ENET.
  - ♦ Supports bisync.
  - ♦ Supports async with the WIC−2A/S, WIC−2T Cards.
  - ♦ Supports 8 Mbps aggregate across 4 ports. Support for speeds above 4 Mbps must use WIC−2T.
  - ♦ WICs are not hot swappable. The network modules support hot swap in the Cisco 3660.
- **General**
  - ♦ There are no configuration rules for these network modules. You can easily exceed the performance of the router by installing multiple Fast Ethernet interfaces.
  - ♦ Time−Division Multiplexing (TDM) support for TDM enabled chassis (Cisco 2600, 3660).
  - ♦ The network modules support hot swap in the Cisco 3660.

Platform Support

Platform	Cisco 2600	Cisco 2600XM	Cisco 3620, Cisco 3640, Cisco 3660	Cisco 3631	Cisco 2691 Cisco 3725 Cisco 3745
NM-1FE2W	not supported	not supported	Cisco IOS versions 12.0(7)XK, 12.1(1)T,12.2,12.2T	not supported	All Cisco IOS versions
NM-1FE1R2W	not supported	not supported	Cisco IOS versions 12.0(7)XK, 12.1(1)T,12.2,12.2T	not supported	All Cisco IOS versions
NM-2FE2W	not supported	not supported	Cisco IOS versions 12.0(7)XK, 12.1(1)T,12.2,12.2T	not supported	All Cisco IOS versions
NM-2W	Cisco IOS versions 12.0(7)XK, 12.1(1)T,12.2,12.2T	Cisco IOS versions 12.2(8)T1	Cisco IOS versions 12.0(7)XK, 12.1(1)T,12.2,12.2T	not supported	All Cisco IOS versions

Note: The Cisco IOS software releases provided are typically the minimum version required to support the platform, module, or feature in question. Use the Software Advisor to choose appropriate software for your network device: match software features to Cisco IOS and CatOS releases, compare IOS releases, or find out which software releases support your hardware. The Software Advisor and other Tools are available in TAC Tools for Access-Dial Technologies.

Configuration

Each interface on the Cisco 2600/3600 series is configured as a slot/unit number. Refer to Overview of Cisco Network Modules for more information on identifying the slot numbers. On the Mixed Media Network Module, the interfaces are addressed as follows:

- The Fast Ethernet interface is **interface fastethernet <slot>/0**.
- The Token Ring interface is **interface tokenring <slot>/0**.
- A serial WIC, a T1 CSU/DSU or a 56/64k channel service unit/data service unit (CSU/DSU) WIC in slot W0 is **interface serial <slot>/0**.
- A BRI-S/T WIC or BRI-U WIC in slot W0 is **interface bri <slot>/0**.
- A serial WIC, a T1 CSU/DSU or a 56/64k CSU/DSU WIC in slot W1 is **interface serial <slot>/0** if slot W0 does not contain a serial port (serial WIC or 56/64k CSU/DSU). If slot W0 has a serial WIC, the serial WIC in slot W1 is **interface serial <slot>/1**.
- A BRI-S/T WIC or BRI-U WIC in slot W1 is **interface bri <slot>/0** if slot W0 does not contain a BRI WIC. If slot W0 has a BRI WIC, the BRI WIC in slot W1 is **interface bri <slot>/1**.
- VWIC interfaces are E1 or T1 controllers. The controller number counts from the lowest WIC slot and lowest controller on the VWIC. Example **controller e1 <slot>/0**.

Related Information

- OIR Support for Analog and Digital Modem Network Modules
- Access Products Support Page
- Access Technology Support Page
- Technical Support – Cisco Systems

Anexo (19)

23458
Paula

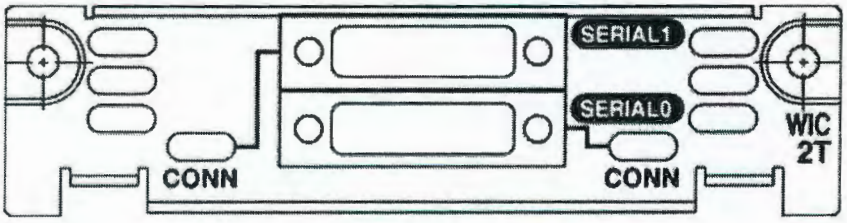
isco – Understanding 2–Port Serial WAN Interface Card (WIC

Table of Contents

Understanding 2-Port Serial WAN Interface Card (WIC-2T)

Introduction

The dual-serial port WAN interface cards (WICs) for the Cisco 2600 and 1700 series 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 is a different physical interface and can support different protocols such as Point-to-Point protocol (PPP) or Frame Relay and Data Terminal Equipment/Data Communications Equipment (DTE/DCE).



Before You Begin

Conventions

For more information on document conventions, see the Cisco Technical Tips Conventions.

Prerequisites

There are no specific prerequisites for this document.

Components Used

This document is not restricted to specific software and hardware versions.

Product Numbers

WIC–2T	2 Port Serial WAN Interface Card

Features

The WIC–2T provides two serial ports using the Smart Serial connector.

- Asynchronous support with a maximum speed (per port) of 115.2 Kbps, minimum 600 bps. If you need to run at speeds lower than 600 bps, use the AUX port instead.
- Synchronous support with a maximum speed of 2.048 Mbps per port.
  - ♦ Supports one port at 8 Mbps when used in NM–1FE1R2W, NM–1FE2W, NM–2FE2W, or NM–2W, or Cisco 2600 chassis WIC slots. All other WIC ports on that network module or Cisco 2600 chassis must not be used.
  - ♦ Supports two ports at 4 Mbps each when used in NM–1FE1R2W, NM–1FE2W, NM–2FE2W, or NM–2W, or Cisco 2600 chassis WIC slots. All other WIC ports on that network module or Cisco 2600 chassis must not be used.
  - ♦ Supports 8 Mbps on all ports simultaneously on 2691, 3725, and 3745. No restrictions. Maximum six ports at 8 Mbps each.

Cables

The WIC–2T serial ports require Smart Serial cables. The following table lists the part number for the cables that can be used with the WIC–2T card.

Cable Type	Product Number	Length	Male/Female
V.35 DTE	CAB–SS–V35MT(=)	10 feet / 3 meters	Male
V.35 DCE	CAB–SS–V35FC(=)	10 feet / 3 meters	Female
RS–232 DTE	CAB–SS–232MT(=)	10 feet / 3 meters	Male
RS–232 DCE	CAB–SS–232FC(=)	10 feet / 3 meters	Female
RS–449 DTE	CAB–SS–449MT(=)	10 feet / 3 meters	Male
RS–449 DCE	CAB–SS–449FC(=)	10 feet / 3 meters	Female
X.21 DTE	CAB–SS–X21MT(=)	10 feet / 3 meters	Male
X.21 DCE	CAB–SS–X21FC(=)	10 feet / 3 meters	Female
EIA–530 DTE	CAB–SS–530MT(=)	10 feet / 3 meters	Male

EIA-530A DTE	CAB-SS-530AMT(=)	10 feet / 3 meters	Male

Platform Support

Platform	Cisco 1600	Cisco 1700	Cisco 2600		Cisco 2600XM		Cisco 3620, 3640, 3660	
Carrier Module	Not Required	Not Required	on-board	NM-2W	on-board	NM-2W	NM-1E2W, NM-1E1R2W, NM-2E2W	NM-1FE2W, NM-1FE1R2W, NM-2FE2W, NM-2W
Cisco IOS® Support	Not supported	All Cisco IOS versions	All Cisco IOS versions	Cisco IOS versions 12.0(7)XK, 12.1(1)T, 12.2, 12.2T	All Cisco IOS versions	Cisco IOS versions 12.2(8)T1	Not supported	Cisco IOS versions 12.0(7)XK, 12.1(1)T, 12.2, 12.2T

The Cisco 1600 Series is not capable of supporting the WIC-2T due to lack of Serial Communications Controllers.

The NM-1E2W, NM-1E1R2W, and NM-2E2W Network Modules do not have enough performance power to support the WIC-2T due to hardware limitations.

Known Problems

The **show version** command shows WIC-2T as "low-speed". This is a display only (cosmetic) problem.

Hardware Failures

The WIC-2T and WIC-2A/S can be damaged by excessive electrostatic discharge. You can minimize this electrostatic discharge in several ways.

- Use shielded cable end-to-end.
- Use a data surge protector that protects against surges over +/- 18v.
- Use an optical isolator (best protection).

Sample Configuration

The following is a sample configuration for the WIC-2T interface card.

Note: There are no **framing**, **clocking** or **linecode** parameters or commands being used here. This is because this card does not have an integrated channel service unit/data service unit (CSU/DSU). You need to use an external CSU/DSU.

Configuration
`maui-soho-02(config)#interface Serial 2/0` `maui-soho-02(config-if)#ip add 10.0.0.1 255.255.255.0`

```
maui-soho-02(config-if)#encapsulation ppp
maui-soho-02(config-if)#no shutdown
```

For more information on configuring the WIC–2T card refer to Configuring Serial Interfaces.

Related Information

- **1– and 2–Port Serial WAN Interface Cards**
- **Overview of Cisco Network Modules**
- **Technical Support – Cisco Systems**

ANEXO 19 A

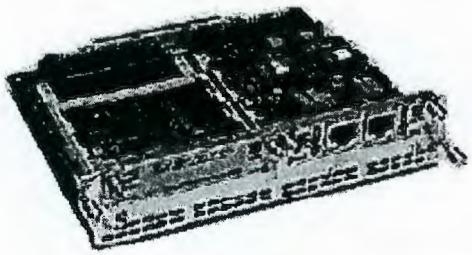
CISCO SYSTEMS

Low Density Voice/Fax Network Modules for the Cisco 2600, 3600 and 3700 Series Routers

Updated August 2002

Cisco 2600, 3600, and 3700 low density voice/fax network modules provide enterprises, managed service providers and service providers the ability to directly connect the PSTN and legacy telephony equipment to existing Cisco 2600, Cisco 3600, and Cisco 3700 routers. This provides immediate multiservice advantages, such as telephony toll bypass, new packet telephony applications, and full gateway integration within a Cisco AVVID architecture.

Figure 1 NM-2V Module with One Two-Port FXO VIC with battery reversal detection and Caller ID support (VIC-2FXO-M1)



The low density voice/fax network modules for the Cisco 2600, 3600, and 3700 series multiservice access routers enable packet voice technologies including VoIP (H.323, MGCP and SIP), VoFR and VoATM (AAL5). Cisco voice solutions provide the means for integrating both voice and data within a single network allowing users to take advantage of services, such as toll-bypass, without sacrificing voice quality. This combination of voice solutions leverages the Cisco proven track record of being able to effectively handle time-sensitive traffic, such as Systems Network Architecture (SNA) over IP networks. Cisco IOS® software also incorporates built-in quality-of-service (QoS) features along with standards-based encapsulation providing efficient direct transport of both voice and fax over IP, Frame Relay and ATM networks. These Cisco IOS solutions enable time-sensitive voice traffic to be moved across even low-bandwidth WAN connections with the priority and quality voice/fax demands. Transporting voice over IP networks continues to provide transport flexibility since IP can be routed across a multitude of WAN technologies (leased lines, Frame Relay, and ATM) along with providing direct connectivity to the desktop.

The low density voice/fax network modules slide into Cisco 2600, 3600, and 3700 network module slots and contain either one or two voice interface card (VIC) slots. The VICs are daughter cards that slide into the voice/fax network modules and provide the interface to the telephony equipment and the PSTN. Just as the Cisco WAN interface cards

can be swapped with other WAN interface cards, the Cisco VICs can be deployed interchangeably with other VICs in the voice/fax network modules. This built-in flexibility and investment protection are key reasons for the world-wide popularity of Cisco modular branch office router products.

VICs currently available include two-port foreign exchange station (FXS), direct inward dial (DID), foreign exchange office (FXO), Centralized Automated Message Accounting (CAMA) and E&M analog interface cards. Also available are a two-port ISDN Basic Rate Interface (BRI) digital interface card providing no phantom power and a two-port ISDN Basic Rate Interface (BRI) digital interface card providing -48V phantom power. These cards cover the entire range of analog connectivity options along with user side Q.931 and QSIG digital BRI connections (see chart). A Cisco 2600 series or 3620 can house one voice/fax module that contains up to two VICs, a Cisco 3640 can house up to three modules with up to a total of six VICs, and the 3660 holds up to six network modules providing a maximum of 24 analog voice ports. In addition, a Cisco 3725 can house two voice/fax modules with a total of four VICs and a Cisco 3745 can house up to four modules with a total of eight VICs.

These low density/fax network modules also provide the gateway to Cisco AVVID architectures for calls to and from the PSTN and legacy telephony equipment (including PBXs, analog telephones, fax machines and key systems). Users can deploy networks which leverage investments in existing legacy telephony equipment while also deploying and integrating IP telephony immediately or in the future. These network modules enable users to operate at any point on the voice, video & data integrated infrastructure spectrum while incrementally adding connections to both legacy telephony and IP telephony on these networks.

Module/VIC	Description
NM-1V	One voice/fax interface card slot network module
NM-2V	Two voice/fax interface card slot network module
VIC-2FXS	Two-port FXS voice/fax interface card
VIC-2FXO	Two-port FXO voice/fax interface card [also see VIC-2FXO-M1]
VIC-2E/M	Two-port E&M voice/fax interface card
VIC-2FXO-EU	Two-port FXO voice/fax interface card (for Europe) [also see VIC-2FXO-M2]
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]
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-2BRI-S/T-TE	Two-port BRI voice/fax interface card (terminal side)
VIC-2BRI-NT/TE	Two-port BRI voice/fax interface card (network and terminal side)
VIC-2DID	Two-port DID (direct inward dial) voice/fax interface card
VIC-2CAMA	Two-port CAMA trunk interface card

Table 1 Cisco Voice Interface Card Applications

VIC Type	Application
VIC-2FXS	Use to connect directly to phones, fax machines, and key systems (generates battery polarity reversal with IOS Plus 12.1.2T and later and generates Caller ID using IOS Plus 12.1.3T or later).
VIC-2FXO	Use to connect to PBX or key system and to provide off-premise connections
VIC-2E/M	Use to connect to PBX or key system trunk lines
VIC-2FXO-EU	Use to connect to PBX or key system and to provide off-premise connections in Europe
VIC-2FXO-M1	Use to connect to PBX or key system and to provide off-premise connections in the U.S., Canada and other countries. Includes support for battery polarity reversal detection and Caller ID (requires Cisco IOS Plus 12.1.2T and later and supports Caller ID using Cisco IOS Plus 12.1.3T or later).
VIC-2FXO-M2	Use to connect to PBX or key system and to provide off-premise connections in Europe. Includes support for battery polarity reversal detection and Caller ID (requires Cisco IOS Plus 12.1.2T or later for battery reversal and supports Caller ID using Cisco IOS Plus 12.1.3T or later)
VIC-2FXO-M3	Use to connect to PBX or key system and to provide off-premise connections in Australia
VIC-2BRI-S/T-TE	Use to connect to PBX or key system and to provide off-premise connections (ISDN voice BRI)
VIC-2BRI-NT/TE	Use to connect as network side to PBX or key system and to provide off-premise connections (ISDN voice BRI)
VIC-2DID	Use to provide off–premise direct-inward-dial connection to CO. Serves only incoming calls from the PSTN. Supports caller ID.
VIC-2CAMA	Use to connect to CAMA trunk to provide E-911 service (North America only)

Feature	Benefit
Voice/Fax over IP	Voice and fax traffic are transport independent, because IP traffic at Layer 3 can travel over any Layer 1 or Layer 2 media, including ISDN, leased lines, serial connections, Frame Relay, Ethernet, Token Ring, and Asynchronous Transfer Mode (ATM).
Voice/Fax over Frame Relay	Applications requiring voice and fax traffic to be routed directly over Frame Relay networks will take advantage of FRF.11 and FRF.12 VoFR and fragmentation standards. This solution also uses features found only in Cisco IOS software for maintaining voice quality. VoIP can also be transported over FR.
Voice over ATM	Transport voice directly over ATM networks using AAL 5 encapsulation. Leverages existing ATM networks as a direct transport method for voice. VoATM requires ATM interfaces such as T1/E1 ATM, IMA, DS3/E3 or OC-3, or DSL WICs. VoIP can also be transported over ATM.
Connection Trunk	Creates a permanent tie-line replacement structure (digital-to-digital, digital-to-analog, or analog-to-analog capabilities).
LVBO (Local Voice Busy-Out)	Automatically busy out any desired voice trunk line to a PBX or PSTN when a direct WAN or LAN connection to the router is down. Also, busy out a far end trunk connection when configured for Connection Trunk.
Caller ID Support	Per-port configurable caller ID to phones connected to analog FXS voice ports using per call un-blocking if desired. Also provide caller ID over analog FXO and DID voice interfaces. Interoperates with analog phones, PSTNs, PBXs, H.323 terminals (i.e. Microsoft Netmeeting), Cisco Call Manager and IP phones.
PSTN Fallback	Uses Service Assurance Agent (SAA) to determine latency, delay and jitter and provide real-time ICPIF calculations before establishing a call across an IP infrastructure. SAA packets emulate voice packets receiving the same priority as voice throughout the entire network. A superior method to data and ping packets for determining congestion levels.
Robust Router-Based Voice Gateway Solution	A single device solution, which reduces management costs, minimizes latency, and has extremely low failure rates, compares favorably with most other voice over IP vendors' PC-based solutions. These solutions still require a LAN router and, therefore, result in not only increased management expenses but also higher PC failure rates.
Modular Architecture	Support any combination of voice and data within a single platform. Allows users to add functionality at any time after deployment.
Voice and Fax over Same Port	Ports can be used for both voice and fax traffic--no dedicated ports are required.
Works with Existing Phones, Faxes, PBXs, and Key Systems	No user retraining is required.
H.323 v3/v2/v1 Compatibility	The Cisco voice/fax modules are interoperable with numerous emerging voice and videoconferencing applications, such as Microsoft NetMeeting, Intel Internet Phone, LAN-based IP telephony equipment, and Cisco Call Manager.
High-Performance DSP Architecture	The Cisco voice/fax modules offer extremely low latency, which is essential for high-quality voice and fax traffic; the DSP architecture also enables all critical functions to be handled in software, which allows for simple code updates, scalability, and new features.
ITU Standards G.729, G.729a/b, G.711, G.723.1, G.726 and G.728	These are standards-based compression technologies allowing transmission of voice across IP, Frame Relay and ATM. G.711 is standard 64 kbps PCM modulation using either u-law or A-law.
Advanced Quality of Service (QoS) Mechanisms	These configurable Cisco IOS features reserve appropriate bandwidth and prioritize voice and fax traffic to ensure transparent delivery of toll-quality voice and fax. They include Resource Reservation Protocol (RSVP), Queuing Techniques (such as Low Latency Queuing), IP Precedence, and DiffServ Code Points.
Compressed Real-Time Protocol (cRTP)	These Cisco IOS features offer RTP header compression and packet fragmentation techniques that allow toll-quality voice and fax transmissions over low-bandwidth (56K and 64K) WAN connections.

Feature	Benefit
Silence Suppression/Voice Activity Detection (VAD)	Bandwidth is used only when someone is speaking. During silent periods of a phone call, bandwidth is available for data traffic.
Comfort Noise Generation	To better simulate phone calls over voice networks, this feature reassures the phone user that the connection is being maintained, even when no voice packets are being transmitted.
Dial Plan Mapping	Automatic mapping of dialed phone numbers to IP addresses simplifies configuration and management.
Dual Tone Multifrequency (DTMF) Tone Processing	This feature enables access to voice-mail and Interactive Voice Response (IVR) systems.
T.30 Protocol Recognition	This feature enables real-time fax capability.
Country-Specific Signaling	This feature transparently delivers customary phone signals to users, facilitating acceptance of new technology.
Autocalling	With this feature, a destination phone can be configured to automatically ring when the handset is lifted (also known as Private Line Automatic Ring-down—PLAR).
Hunt Groups	Calls can be forwarded automatically to the first available line.
Battery Polarity Reversal Detection and Initiation	Detection of disconnect supervision and far-end answer supervision via battery polarity reversal provides a robust method of providing supervisory disconnect especially for loop start signaling on FXS and FXO interfaces (12.1(2)T and later Cisco IOS Plus images support battery polarity reversal on the VIC-2FXS, VIC-2FXO-M1 and VIC-2FXO-M2 VICs).
Supervisory Disconnect	Signalling protocols such as loop-start do not provide means for quickly detecting when the call initiation is terminated prior to call connection. Supervisory disconnect quickly makes this determination and frees valuable resources for other calls.
ISDN BRI Network Side and Phantom Power	Cisco IOS software releases 12.1.5T provide the ability to connect PBX configured as user side directly to the router. Phantom power is also provided to accommodate equipment that requires it.
CAMA trunk connection	Cisco IOS software release 12.2(11)T provides the ability to connect to analog CAMA trunk wich allows E-911 services.

Software and Memory Requirements

Product	Cisco IOS Software Version		
	Cisco 2600	Cisco 3600	Cisco 3700
NM-1V	11.3(4)T or later 12.0(1)T or later	11.3(1)T or later 12.0(1)T or later	12.2.(8)T or later
NM-2V	11.3(4)T or later 12.0(1)T or later	11.3(1)T or later 12.0(1)T or later	12.2.(8)T or later
VIC-2FXS	11.3(4)T or later 12.0(1)T or later	11.3(1)T or later 12.0(1)T or later	12.2.(8)T or later
VIC-2FXO	11.3(4)T or later 12.0(1)T or later	11.3(1)T or later 12.0(1)T or later	12.2.(8)T or later
VIC-2E/M[1]	11.3(4)T or later 12.0(1)T or later	11.3(1)T or later 12.0(1)T or later	12.2.(8)T or later
VIC-2FXO-EU	11.3(6)T or later 12.0(2)T or later	11.3(6)T or later 12.0(2)T or later	12.2.(8)T or later
VIC-2FXO-M1	12.1(2)T or later	12.1(2)T or later	12.2.(8)T or later
VIC-2FXO-M2	12.1(2)T or later	12.1(2)T or later	12.2.(8)T or later
VIC-2FXO-M3	11.3(6)T or later 12.0(2)T or later	11.3(6)T or later 12.0(2)T or later	12.2.(8)T or later
VIC-2BRI-S/T-TE	12.0(3)T or later	12.0(3)T or later 3660 requires 12.1.2T	12.2.(8)T or later
VIC-2BRI-NT/TE	12.1.(3)X1 or later 12.1.(5)T or later	12.1.(3)X1 or later 12.1.(5)T or later	12.2.(8)T or later
VIC-2DID	12.1(5)XM1 or later 12.2(2)T or later	12.1(5)XM1 or later 12.2(2)T or later	12.2.(8)T or later
VIC-2CAMA	12.2.(11)T or later	12.2.(11)T or later	12.2.(11)T or later

1. The VIC-2E/M requires Cisco IOS Plus version 11.3(6)T for on-premise connections in Australia.

Product	Software Image	Image Name	Flash Requirements	DRAM Requirements
Cisco 2600	ENTERPRISE/SNASW PLUS IPSEC 56	c2600-a3jk8s-mz	16MB	48MB
Cisco 2600	ENTERPRISE/SNASW PLUS IPSEC 3DES	c2600-a3jk9s-mz	16MB	48MB
Cisco 2600	ENTERPRISE/SNASW PLUS	c2600-a3js-mz	16MB	48MB
Cisco 2600	IP/IPX/AT/DEC/FW/IDS PLUS	c2600-do3s-mz	16MB	48MB
Cisco 2600	IP/IPX/AT/DEC PLUS	c2600-ds-mz	16MB	40MB
Cisco 2600	IP/FW/IDS PLUS IPSEC 56	c2600-ik8o3s-mz	16MB	48MB
Cisco 2600	IP PLUS IPSEC 56	c2600-ik8s-mz	16MB	40MB
Cisco 2600	IP/FW/IDS PLUS IPSEC 3DES	c2600-ik9o3s-mz	16MB	48MB
Cisco 2600	IP PLUS IPSEC 3DES	c2600-ik9s-mz	16MB	40MB
Cisco 2600	IP PLUS	c2600-is-mz	16MB	40MB
Cisco 2600	ENTERPRISE/FW/IDS PLUS IPSEC 56	c2600-jk8o3s-mz	16MB	48MB
Cisco 2600	ENTERPRISE PLUS IPSEC 56	c2600-jk8s-mz	16MB	48MB
Cisco 2600	ENTERPRISE/FW/IDS PLUS IPSEC 3DES	c2600-jk9o3s-mz	16MB	48MB
Cisco 2600	ENTERPRISE PLUS IPSEC 3DES	c2600-jk9s-mz	16MB	48MB
Cisco 2600	ENTERPRISE PLUS	c2600-js-mz	16MB	48MB
Cisco 2600	ENTERPRISE PLUS/H323 MCM	c2600-jsx-mz	16MB	64MB

Note that the default Flash is 8MB and default DRAM is 32MB on 2600 series shipments configured with Cisco IOS 12.2(1).

The Flash and DRAM requirements above are for the Cisco IOS Plus 12.2(1) release. The actual requirement may vary depending on the version of Cisco IOS software used (refer to the release notes for the version of Cisco IOS software being used for exact FLASH and DRAM requirements).

Product	Software Image	Image Name	Flash Requirements	DRAM Requirements
Cisco 3620	ENTERPRISE/SNASW PLUS IPSEC 56	c3620-a3jk8s-mz	16MB	64MB
Cisco 3620	ENTERPRISE/SNASW PLUS IPSEC 3DES	c3620-a3jk9s-mz	16MB	64MB
Cisco 3620	ENTERPRISE/SNASW PLUS	c3620-a3js-mz	16MB	64MB
Cisco 3620	IP/IPX/AT/DEC/FW/IDS PLUS	c3620-do3s-mz	16MB	64MB
Cisco 3620	IP/IPX/AT/DEC PLUS	c3620-ds-mz	16MB	48MB
Cisco 3620	IP/FW/IDS PLUS IPSEC 56	c3620-ik8o3s-mz	16MB	64MB
Cisco 3620	IP PLUS IPSEC 56	c3620-ik8s-mz	16MB	48MB

Product	Software Image	Image Name	Flash Requirements	DRAM Requirements
Cisco 3620	IP/FW/IDS PLUS IPSEC 3DES	c3620-ik9o3s-mz	16MB	64MB
Cisco 3620	IP PLUS IPSEC 3DES	c3620-ik9s-mz	16MB	48MB
Cisco 3620	IP PLUS	c3620-is-mz	16MB	48MB
Cisco 3620	ENTERPRISE/FW/IDS PLUS IPSEC 56	c3620-jk8o3s-mz	16MB	64MB
Cisco 3620	ENTERPRISE PLUS IPSEC 56	c3620-jk8s-mz	16MB	64MB
Cisco 3620	ENTERPRISE/FW/IDS PLUS IPSEC 3DES	c3620-jk9o3s-mz	16MB	64MB
Cisco 3620	ENTERPRISE PLUS IPSEC 3DES	c3620-jk9s-mz	16MB	64MB
Cisco 3620	ENTERPRISE PLUS	c3620-js-mz	16MB	64MB
Cisco 3620	ENTERPRISE PLUS/H323 MCM	c3620-jsx-mz	16MB	64MB

Note that the default Flash is 8MB and default DRAM is 32MB on 3620 series shipments configured with Cisco IOS 12.2(1).

The Flash and DRAM requirements above are for the Cisco IOS Plus 12.2(1) release. The actual requirement may vary depending on the version of Cisco IOS software used (refer to the release notes for the version of Cisco IOS software being used for exact FLASH and DRAM requirements).

Product	Software Image	Image Name	Flash Requirements	DRAM Requirements
Cisco 3640	ENTERPRISE/SNASW PLUS IPSEC 56	c3640-a3jk8s-mz	16MB	64MB
Cisco 3640	ENTERPRISE/SNASW PLUS IPSEC 3DES	c3640-a3jk9s-mz	16MB	64MB
Cisco 3640	ENTERPRISE/SNASW PLUS	c3640-a3js-mz	16MB	64MB
Cisco 3640	IP/IPX/AT/DEC/FW/IDS PLUS	c3640-do3s-mz	16MB	64MB
Cisco 3640	IP/IPX/AT/DEC PLUS	c3640-ds-mz	16MB	48MB
Cisco 3640	IP/FW/IDS PLUS IPSEC 56	c3640-ik8o3s-mz	16MB	64MB
Cisco 3640	IP PLUS IPSEC 56	c3640-ik8s-mz	16MB	48MB
Cisco 3640	IP/FW/IDS PLUS IPSEC 3DES	c3640-ik9o3s-mz	16MB	64MB
Cisco 3640	IP PLUS IPSEC 3DES	c3640-ik9s-mz	16MB	48MB
Cisco 3640	IP PLUS	c3640-is-mz	16MB	48MB
Cisco 3640	ENTERPRISE/FW/IDS PLUS IPSEC 56	c3640-jk8o3s-mz	16MB	64MB
Cisco 3640	ENTERPRISE PLUS IPSEC 56	c3640-jk8s-mz	16MB	64MB
Cisco 3640	ENTERPRISE/FW/IDS PLUS IPSEC 3DES	c3640-jk9o3s-mz	16MB	64MB
Cisco 3640	ENTERPRISE PLUS IPSEC 3DES	c3640-jk9s-mz	16MB	64MB

Product	Software Image	Image Name	Flash Requirements	DRAM Requirements
Cisco 3640	ENTERPRISE PLUS	c3640-js-mz	16MB	64MB
Cisco 3640	ENTERPRISE PLUS/H323 MCM	c3640-jsx-mz	16MB	64MB

Note that the default Flash is 8MB and default DRAM is 32MB on 3640 series shipments configured with Cisco IOS 12.2(1).

The Flash and DRAM requirements above are for the Cisco IOS Plus 12.2(1) release. The actual requirement may vary depending on the version of Cisco IOS software used (refer to the release notes for the version of Cisco IOS software being used for exact FLASH and DRAM requirements).

Product	Software Image	Image Name	Flash Requirements	DRAM Requirements
Cisco 3660	ENTERPRISE/SNASW PLUS IPSEC 56	c3660-a3jk8s-mz	16MB	64MB
Cisco 3660	ENTERPRISE/SNASW PLUS IPSEC 3DES	c3660-a3jk9s-mz	16MB	64MB
Cisco 3660	ENTERPRISE/SNASW PLUS	c3660-a3js-mz	16MB	64MB
Cisco 3660	IP/IPX/AT/DEC/FW/IDS PLUS	c3660-do3s-mz	16MB	64MB
Cisco 3660	IP/IPX/AT/DEC PLUS	c3660-ds-mz	16MB	64MB
Cisco 3660	IP/FW/IDS PLUS IPSEC 56	c3660-ik8o3s-mz	16MB	64MB
Cisco 3660	IP PLUS IPSEC 56	c3660-ik8s-mz	16MB	64MB
Cisco 3660	IP/FW/IDS PLUS IPSEC 3DES	c3660-ik9o3s-mz	16MB	64MB
Cisco 3660	IP PLUS IPSEC 3DES	c3660-ik9s-mz	16MB	64MB
Cisco 3660	IP PLUS	c3660-is-mz	16MB	64MB
Cisco 3660	ENTERPRISE/FW/IDS PLUS IPSEC 56	c3660-jk8o3s-mz	16MB	64MB
Cisco 3660	ENTERPRISE PLUS IPSEC 56	c3660-jk8s-mz	16MB	64MB
Cisco 3660	ENTERPRISE/FW/IDS PLUS IPSEC 3DES	c3660-jk9o3s-mz	16MB	64MB
Cisco 3660	ENTERPRISE PLUS IPSEC 3DES	c3660-jk9s-mz	16MB	64MB
Cisco 3660	ENTERPRISE PLUS	c3660-js-mz	16MB	64MB
Cisco 3660	ENTERPRISE PLUS/H323 MCM	c3660-jsx-mz	16MB	64MB

Note that the default Flash is 8MB and default DRAM is 32MB on 3660 series shipments configured with Cisco IOS 12.2(1).

The Flash and DRAM requirements above are for the Cisco IOS Plus 12.2(1) release. The actual requirement may vary depending on the version of Cisco IOS software used (refer to the release notes for the version of Cisco IOS software being used for exact FLASH and DRAM requirements).

Product	Software Image	Image Name	Flash Requirements	DRAM Requirements
Cisco 3725	IP/IPX/AT/FW/IDS PLUS	c3725-bino3s-mz	32MB	128MB
Cisco 3725	IP/IPX/AT PLUS	c3725-bins-mz	32MB	128MB
Cisco 3725	IP/FW/IDS PLUS IPSEC 3DES	c3725-ik9o3s-mz	32MB	128MB
Cisco 3725	IP PLUS IPSEC 3DES	c3725-ik9s-mz	32MB	128MB
Cisco 3725	IP PLUS	c3725-is-mz	32MB	128MB
Cisco 3725	ENTERPRISE/FW/IDS PLUS IPSEC 3DES	c3725-jk9o3s-mz	32MB	128MB
Cisco 3725	ENTERPRISE PLUS IPSEC 3DES	c3725-jk9s-mz	32MB	128MB
Cisco 3725	ENTERPRISE PLUS	c3725-js-mz	32MB	128MB
Cisco 3725	ENTERPRISE PLUS/H323 MCM	c3725-jsx-mz	32MB	128MB

Note that the default Flash is 32MB and default DRAM is 128MB on 3725 series shipments configured with Cisco IOS 12.2(8)T.

The Flash and DRAM requirements above are for the Cisco IOS Plus 12.2(8)T release. The actual requirement may vary depending on the version of Cisco IOS software used (refer to the release notes for the version of Cisco IOS software being used for exact FLASH and DRAM requirements).

Product	Software Image	Image Name	Flash Requirements	DRAM Requirements
Cisco 3745	IP/IPX/AT/FW/IDS PLUS	c3745-bino3s-mz	32MB	128MB
Cisco 3745	IP/IPX/AT PLUS	c3745-bins-mz	32MB	128MB
Cisco 3745	IP/FW/IDS PLUS IPSEC 3DES	c3745-ik9o3s-mz	32MB	128MB
Cisco 3745	IP PLUS IPSEC 3DES	c3745-ik9s-mz	32MB	128MB
Cisco 3745	IP PLUS	c3745-is-mz	32MB	128MB
Cisco 3745	ENTERPRISE/FW/IDS PLUS IPSEC 3DES	c3745-jk9o3s-mz	32MB	128MB
Cisco 3745	ENTERPRISE PLUS IPSEC 3DES	c3745-jk9s-mz	32MB	128MB
Cisco 3745	ENTERPRISE PLUS	c3745-js-mz	32MB	128MB
Cisco 3745	ENTERPRISE PLUS/H323 MCM	c3745-jsx-mz	32MB	128MB

Note that the default Flash is 32MB and default DRAM is 128MB on 3745 series shipments configured with Cisco IOS 12.2(8)T.

The Flash and DRAM requirements above are for the Cisco IOS Plus 12.2(8)T release. The actual requirement may vary depending on the version of Cisco IOS software used (refer to the release notes for the version of Cisco IOS software being used for exact FLASH and DRAM requirements).

Specifications

NM-1V	One voice/fax interface card slot network module
Cisco IOS Requirement	11.3(1)T or later for Cisco 3600 11.3(4)T or later for Cisco 2600 12.2(8)T or later for Cisco 2691 and 3700
Cisco Part Number	800-02489-01
FCC Specifications	FCC Class B device
Spare	NM-1V=
Mean Time between Failures (MTBF)	946,423 hours
Requires One VIC	VIC-2FXS 800-02493-01 VIC-2FXO 800-02495-01 VIC-2E/M 800-02497-01 VIC-2FXO-EU 800-03639-01 VIC-2FXO-M1 800-05298-01 VIC-2FXO-M2 800-05920-01 VIC-2FXO-M3 800-04581-01 VIC-2BRI-S/T-TE 800-03803-1 VIC-2BRI-NT/TE 800-07272-01 VIC-2DID 800-06487-01 VIC-2CAMA 800-18443-01

NM-2V	Two voice/fax interface card slot network module
Cisco IOS Requirement	11.3(1)T or later for Cisco 3600 11.3(4)T or later for Cisco 2600 12.2(8)T or later for Cisco 2691 and 3700
Cisco Part Number	800-02491-01
FCC Specifications	FCC Class B device
Spare	NM-2V=
MTBF	755,717 hours
Requires at Least One VIC (maximum of two)	VIC-2FXS 800-02493-01 VIC-2FXO 800-02495-01 VIC-2E/M 800-02497-01 VIC-2FXO-EU 800-03639-01 VIC-2FXO-M1 800-05298-01 VIC-2FXO-M2 800-05920-01 VIC-2FXO-M3 800-04581-01 VIC-2BRI-S/T-TE 800-03803-1 VIC-2BRI-NT/TE 800-07272-01 VIC-2DID 800-06487-01 VIC-2CAMA 800-18443-01

VIC-2FXS	Two-port FXS voice/fax interface card
Interface Type	Foreign exchange station
Cisco IOS Requirement	11.3(1)T or later for Cisco 3600 11.3(4)T or later for Cisco 2600 12.2(8)T or later for Cisco 2691 and 3700
Cisco Part Number	800-02493-01
Compliance	FCC Class B device, CE
Safety Conformance	UL1950
Spare	VIC-2FXS=
Address Signaling Formats	In-band DTMF Out-of-band pulse (10/20 pps)
Signaling Formats	Loop start, ground start
Ringing Tone	Configurable for different country requirements
Ringing Voltage	<45 Vrms at 5 REN at 25 Hz (configurable frequency)
Ringing Frequencies	20 Hz, 50 Hz
Physical Connector	RJ-11
Number of Connectors/Ports	Two
MTBF	2,248,909 hours

VIC-2FXO	Two-port FXO voice/fax interface card
Interface Type	Foreign exchange office
Cisco IOS Requirement	11.3(1)T or later for Cisco 3600 11.3(4)T or later for Cisco 2600 12.2(8)T or later for Cisco 2691 and 3700
Cisco Part Number	800-02497-01
Compliance	FCC Class B device, CE
Safety Conformance	UL1950
Spare	VIC-2FXO=
Signaling Formats	Loop start, ground start
Address Signaling Formats	In-band DTMF Out-of-band pulse (10/20 pps)
Tone Disconnect Supervision	Call disconnect on progress tone of less than 600 Hz
Power Interrupt Disconnect	Call disconnect on power interrupt of > 600 msec
Physical Connector	RJ-11
Number of Connectors/Ports	Two
MTBF	2,302,609 hours

VIC-2E/M	Two-port E&M voice/fax interface card
Interface Type	For PBX trunking
Cisco IOS Requirement	11.3(1)T or later for Cisco 3600 11.3(4)T or later for Cisco 2600 12.2(8)T or later for Cisco 2691 and 3700
Cisco Part Number	800-02497-01
Compliance	FCC Class B device, CE
Safety Conformance	UL 1950
Spare	VIC-2E/M=
Address Signaling Formats	In-band DTMF Out-of-band pulse (10/20 pps)
Signaling Formats	Immediate, delay dial, wink start
Signaling Types	I, II, III, and V
E-Lead Current Limit	100 mA
M-Lead Sensitivity	> 3 mA
Pulse Distortion	< 2%
Physical Connector	4 wire/2 wire
Number of Connectors/Ports	Two
MTBF	1,943,521 hours

VIC-2FXO-EU	Two-port FXO voice/fax interface card (for Europe)
Interface Type	Foreign exchange office
Cisco IOS Requirement	11.3(6)T or later for Cisco 3600 or 12.0(2)T or later for Cisco 3600 11.3(6)T or later for Cisco 2600 or 12.0(2)T or later for Cisco 3600 12.2(8)T or later for Cisco 2691 and 3700
Cisco Part Number	800-03639-01
Compliance	CE, CTR-21
Safety Conformance	UL1950
Spare	VIC-2FXO-EU=
Signaling Formats	Loop start
Address Signaling Formats	In-band DTMF Out-of-band pulse (10/20 pps)
Tone Disconnect Supervision	Call disconnect on progress tone of less than 600 Hz
Power Interrupt Disconnect	Call disconnect on power interrupt of > 600 msec
Physical Connector	RJ-11
Number of Connectors/Ports	Two
MTBF	1,010,264 hours

VIC-2FXO-M1	Two-port FXO voice/fax interface card with battery reversal detection and caller ID (for US, Canada, Japan and other countries)
Interface Type	Foreign exchange office
Cisco IOS Requirement	12.1.2T or later for Cisco 3600 and 2600 12.2(8)T or later for Cisco 2691 and 3700
Cisco Part Number	800-05298-01
Compliance	FCC Class B device, CE
Safety Conformance	UL1950
Spare	VIC-2FXO-M1=
Signaling Formats	Loop start, ground start
Address Signaling Formats	In-band DTMF Out-of-band pulse (10/20 pps)
Tone Disconnect Supervision	Call disconnect on progress tone of less than 600 Hz
Battery Polarity Reversal Detection	Detection of disconnect supervision and far-end answer supervision via battery polarity reversal
Power Interrupt Disconnect	Call disconnect on power interrupt of > 600 msec
Physical Connector	RJ-11
Number of Connectors/Ports	Two
MTBF	546,560 hours (using Bellcore model)

VIC-2FXO-M2	Two-port FXO voice/fax interface card with battery reversal detection and caller ID support (for Europe)
Interface Type	Foreign exchange office
Cisco IOS Requirement	12.1.2T or later for Cisco 3600 and 2600 12.2(8)T or later for Cisco 2691 and 3700
Cisco Part Number	800-05920-01
Compliance	CE, CTR-21
Safety Conformance	UL1950
Spare	VIC-2FXO-M2=
Signaling Formats	Loop start
Address Signaling Formats	In-band DTMF Out-of-band pulse (10/20 pps)
Tone Disconnect Supervision	Call disconnect on progress tone of less than 600 Hz
Battery Polarity Reversal Detection	Detection of disconnect supervision and far-end answer supervision via battery polarity reversal
Power Interrupt Disconnect	Call disconnect on power interrupt of > 600 msec
Physical Connector	RJ-11
Number of Connectors/Ports	Two
MTBF	656, 116 hours (using Bellcore model)

VIC-2FXO-M3	Two-port FXO voice/fax interface card (for Australia)
Interface Type	Foreign exchange office
Cisco IOS Requirement	11.3(6)T or later for Cisco 3600 or 12.0(2)T or later for Cisco 3600 11.3(6)T or later for Cisco 2600 or 12.0(2)T or later for Cisco 2600 12.2(8)T or later for Cisco 2691 and 3700
Cisco Part Number	800-04581-01
Compliance	AUA TS.002, AUA TS.003
Safety Conformance	UL1950
Spare	VIC-2FXO-M3=
Signaling Formats	Loop start, ground start
Address Signaling Formats	In-band DTMF Out-of-band pulse (10/20 pps)
Tone Disconnect Supervision	Call disconnect on progress tone of less than 600 Hz
Power Interrupt Disconnect	Call disconnect on power interrupt of > 600 msec
Physical Connector	RJ-11
Number of Connectors/Ports	Two
MTBF	1,010,264 hours

VIC-2BRI-ST-TE	Two-port BRI voice/fax interface card (terminal side)
Interface Type	ISDN Basic Rate Interface
Cisco IOS Requirement	12.0(3)T or later for Cisco 3600 and 2600 12.2(8)T or later for Cisco 2691 and 3700
Cisco Part Number	800-03803-01
Compliance	FCC Part 68 CS03 CTR3 TS-031 JATE Green Book
Safety Conformance	UL1950, CAN/CSA-C22.2, IEC 950, EN60950
Spare	VIC-2BRI-ST-TE=
ITU Compliance	ITU-T Q.920, Q.921, Q.930, Q.931
Interface	Four wire user side S/T
ISDN Digital Access	Basic Rate Interface (BRI) 4B+2D
Physical Connector	RJ-45
Number of Connectors/Ports	Two
MTBF	2,951,544 hours

VIC-2BRI-NT/TE	Two-port BRI voice/fax interface card (network side)
Interface Type	ISDN Basic Rate Interface
Cisco IOS Requirement	12.1(3)XI or 12.1(5)T later for Cisco 3600 and 2600 12.2(8)T or later for Cisco 2691 and 3700
Cisco Part Number	800-07272-01
Compliance	FCC Part 68 CS03 CTR3 TS-031 JATE Green Book
Safety Conformance	UL1950, CAN/CSA-C22.2, IEC 950, EN60950
Spare	VIC-2BRI-NT/TE=
ITU Compliance	ITU-T Q.920, Q.921, Q.930, Q.931
Interface	Four wire user side S/T or network side NT
ISDN Digital Access	Basic Rate Interface (BRI) 4B+2D
Physical Connector	RJ-45
Number of Connectors/Ports	Two
MTBF	1,991,520 hours

VIC-2DID	Two-port DID voice/fax interface card
Interface Type	Direct inward dial trunk
Cisco IOS Requirement	12.1(5)XM1 or 12.2(2)T later for Cisco 2600/3600 12.2(8)T or later for Cisco 2691 and 3700
Cisco Part Number	800-06487-01
Compliance	FCC Class B device, CE
Safety Conformance	UL1950
Spare	VIC-2DID=
Address Signaling Formats	In-band DTMF Out-of-band pulse (10/20 pps)
Signaling Formats	Immediate, delay dial, wink start
Disconnect Supervision	Power denial (Calling Party Control, far-end disconnect)
Caller ID	On-hook transmission of FSK data
Physical Connector	RJ-11
Number of Connectors/Ports	Two
MTBF	3,270,000 hours

VIC-2CAMA	Two-port CAMA trunk interface card (user side)
Interface Type	CAMA trunk
Cisco IOS Requirement	12.2(11)T or later for Cisco 2600, 3600, and 3700
Cisco Part Number	800-18443-1
Compliance	FCC Part 68
Safety Conformance	UL1950, CAN/CSA-C22.2
Spare	VIC-2CAMA=
Signaling Format	wink
Battery Polarity Reversal Detection	Detection of disconnect supervision via battery polarity reversal
Physical Connector	RJ-11
Number of Connectors/Ports	Two
MTBF	613,250 hours

Homologation

The following VICs are approved for the countries listed below for off-premise and on-premise connections.

VIC-2FXO	VIC-2FXO-EU	VIC-2FXO-M1	VIC-2FXO-M2	VIC-2FXO-M3	VIC-2BRI-S/T-TE	VIC-2BRI-NT/TE	VIC-2DID
USA Canada Hong Kong New Zealand Japan Malaysia Taiwan Bulgaria Hungary Russia India Mexico	CE countries* Saudi Arabia Belarus	USA Canada Singapore Poland Hong Kong New Zealand Japan Malaysia China India	CE countries* UAE Bulgaria Israel	Australia	USA Canada Australia Singapore Poland CE countries* Hong Kong New Zealand Japan Malaysia Romania Saudi Arabia Taiwan UAE Belarus Bulgaria Hungary Israel China Czech Republic Russia	USA Canada Australia Singapore Poland CE countries* Hong Kong New Zealand Japan	USA Canada Australia CE countries* Hong Kong **VIC-2CAMA** USA Canada

*European Community countries: Austria, Belgium, Denmark, Finland, France, Germany, Greece, Ireland, Italy, Luxemborg, Netherlands, Portugal, Spain, Sweden, United Kingdom.

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 Australia, Pty., Ltd
Level 9, 80 Pacific Highway
P.O. Box 469
North Sydney
NSW 2060 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 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

ANEXO (198)

Close Window

Toolkit: Feedback

Paula 23413

Cisco Feature Navigator II

Search by Feature | Search by Release | Compare Images

Objective: Define a specific software image in order to view its supported features.

Select from the pull down menus to find releases which support particular platform and feature set combinations.View your results in the table below and repeat as necessary to define a specific software image.

Your Selections:

Platform	**3745**
Major Release	12.3
Release	12.3(1)
Feature Set	ENTERPRISE PLUS IPSEC 3DES

Software usado.

New Search

Search Results

Image Info

Image Name (Dram/Flash) :	c3745-jk9s-mz.12.3-1 (128/32)
Enterprise Product Number :	S374AK9-12301 S374AK9-12301=

This image has software advisories associated with it.Click here for details.
Get This Image Compare Images View MIBs Release Notes

Features

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
Adaptive 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
AppleTalk 1 and 2
AppleTalk Control Protocol (ATCP)

AppleTalk Load Balancing
AppleTalk Remote Access Protocol (ARAP)
AppleTalk Routing over ISL and IEEE 802.10 in Virtual LANs
AppleTalk Update-Based Routing Protocol (AURP)
Asynchronous Line Monitoring
Asynchronous Rotary Line Queuing
Asynchronous Serial Traffic Over UDP
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
AutoSecure
Bandwidth Allocation Control Protocol (BACP)
BGP
BGP 4 OK
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 Information
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
Connection-Mode Network Service (CMNS)
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)
CUG Selection Facility Suppress Option
Custom Queueing (CQ)
Customer Profile Idle Timer Enhancements for Interesting Traffic
DECnet Accounting
DECNet IV
DECnet over ISL
DECnet over LANE
DECNet V
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
Dialer profiles
Dialer Watch
Dialer Watch Connect Delay
Diffie-Hellman Group 5
Diffserv Compliant WRED
Digital J1 Voice Support
Direct Inward Dial (DID)
Disabling LANE Flush Process
Display SAP by Name
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
DLSw+ SNA Type of Service
DLSw+ Support For Transporting LLC1 UI Traffic
DNS based X.25 routing
DNS Lookups over an IPv6 Transport
Double Authentication
Down Stream Physical Unit (DSPU) over DLSw+
Downstream PU concentration (DSPU)
DRP Server Agent

DTMF Events Through SIP Signaling
Dynamic Multiple Encapsulation for Dial-in over ISDN
Dynamic Multipoint VPN (DMVPN)
E1 R2 Signaling
Easy IP (Phase 1)
Easy VPN Remote Enhancements
Easy VPN Server
EIGRP Nonstop Forwarding (NSF) Awareness
Encrypted Kerberized Telnet
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)
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)
Frame Relay Fragmentation with Hardware Compression
Frame Relay FRF.9 Payload Compression
Frame Relay IP RTP Priority
Frame Relay Point-Multipoint Wireless
Frame Relay PVC Interface Priority Queueing
Frame Relay Queuing and Fragmentation at the Interface
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 Tunnel Switching
Frame Relay Voice Adaptive Traffic Shaping
FUNI Support for Routers
FXO Answer and Disconnect Supervision
Gatekeeper Ecosystem Interoperability
Gateway Codec Order Preservation and Shutdown Control
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.323 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
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 IS-IS Multi-Topology Support for IPv6
Integrated IS-IS Nonstop Forwarding Awareness
Integrated IS-IS Point to Point Adjacency over Broadcast Media
Integrated IS-IS support for IPv6

Integrated routing and bridging (IRB)
Inter-Domain Gateway Security Enhancement
Interactive Voice Response (IVR) Version 2.0
Interface Alias Long Name Support
Interface Index Display
Interface Index Persistence
Interface Range Specification
Internal Cause Code Consistency between SIP and H.323
Interworking Signaling Enhancements for H.323 and SIP VoIP
Inverse Multiplexing over ATM (IMA)
IP DSCP marking for Frame-Relay PVC
IP Enhanced IGRP Route Authentication
IP Header Compression Enhancement - PPPoATM and PPPoFR Support
IP Multicast Load Splitting across Equal-Cost Paths
IP Multicast Multilayer Switching (MLS)
IP Multilayer Switching (IP MLS)
IP Named Access Control List
IP over CLNS tunnel
IP Precedence Accounting
IP Precedence for GRE Tunnels
IP Routing
IP RTP Priority
IP Summary Address for RIPv2
IP to ATM CoS, per-VC WFQ and CBWFQ
IP-to-ATM CoS
IPSec MIB Support for Cisco IPSec VPN Management
IPsec 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
IPX Access Control List Violation Logging
IPX Access List Plain English Filters
IPX Control Protocol
IPX Encapsulation for 802.10 VLAN
IPX Multilayer Switching
IPX Named Access Lists
IPX Routing over ISL Virtual LANs
IPX SAP-after-RIP
IPXWAN 2.0
IS-IS
IS-IS Multiarea Support
ISDN
ISDN Advice of Charge (AOC)

ISDN Caller ID Callback
ISDN 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
ISO CLNS
IVR: Enhanced Multilanguage Support
Kerberos V client 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 Circuits
Local Area Transport (LAT)
Local Voice Busyout (LVBO)
Lock and Key
Low Latency Queueing (LLQ)
Low Latency Queueing (LLQ) for Frame Relay
Low Latency Queueing (LLQ) with Priority Percentage Support
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 Networks
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
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 (Multiprotocol Label Switching)
MPLS Class of Service (CoS)
MPLS Class of Service (CoS) Enhancements
MPLS Egress NetFlow Accounting
MPLS Label Distribution Protocol (LDP)
MPLS over ATM: Virtual Circuit (VC) Merge
MPLS Scalability Enhancements for LSC and ATM LSR
MPLS Traceroute
MPLS Traffic Engineering (TE)
MPLS Traffic Engineering (TE) - Automatic bandwidth adjustment for TE tunnels
MPLS Traffic Engineering (TE) - OSPF Support
MPLS Virtual Private Networks (VPN)
MPLS VPN - Inter-Autonomous System Support
MPLS VPN - OSPF PE-CE Support
MPLS VPN Carrier Supporting Carrier
MPLS VPN Carrier Supporting Carrier - IPv4 BGP Label Distribution
MPLS VPN ID
MPLS VPN Inter-AS - IPv4 BGP Label Distribution.
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
Multiprotocol over ATM (MPOA)
Multiprotocol over ATM for Token Ring (MPOA)
Multiservice IP-to-IP Gateway with Media Flow-Around
Named Method Lists for AAA Authorization and Accounting
NAT - Protocol Translation (NAT-PT)
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
NetBEUI over PPP (NBFCP)
Netflow
NetFlow Aggregation
NetFlow BGP Next Hop Support
NetFlow Multicast Support
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
Novell IPX
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
PGM Host
PGM Router Assist
PIM Dense Mode State Refresh
PIM MIB Extension for IP Multicast
PIM Multicast Scalability
PIM Version 1
PIM Version 2
PKI Integration with AAA Server
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
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 Enhancements

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)
Rate Queues for SVC's per sub-interface
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
Rotating 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
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
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
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: Accept-Language Header Support
SIP: Core SIP Technology Enhancements
SIP: Hold Timer Support
SIP: ISDN Suspend/Resume Support
Snapshot routing
OK SNMP (Simple Network Management Protocol)
SNMP Inform Request
SNMP Manager
SNMP Notification Logging
SNMP Support for IOS vLAN Subinterfaces
SNMP Support for vLAN (ISL, DOT1Q) Subinterfaces
SNMP Support over VPN
OK SNMP Version 3
OK SNMPv2C
Software IPPCP (LZS) with Hardware Encryption
Source Interface Selection for Outgoing Traffic with Certificate Authority (CA)
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 Call Agent Driven Fax for Cisco IOS Gateways
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 Intercept
TCP Window Scaling
Telephony Gateway Registration Protocol (TGREP) on Cisco IOS Gateways
Time-Based Access Lists Using Time Ranges
Timer and Retry Enhancements for L2TP and L2F
TN3270
Token Ring ISL
Token Ring LANE
Traffic Policing
Transparent Bridging
Transparent CCS and Frame Forwarding Enhancements
Transparent Common Channel Signaling (T-CCS)
Triggered RIP
Trimble Palisade NTP Synchronization Driver
Trunk Conditioning for FRF.11 and Cisco Trunks
Trusted Root Certification Authority
Trustpoint CLI
Tunnel Endpoint Discovery
Tunnel Type of Service (TOS)
Tunneling of Asynchronous Security Protocols
Turbo Flooding of UDP Datagrams
Two-Rate Policer
UDLR Tunnel ARP and IGMP Proxy
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.120 Support
V.92 Modem on Hold
V.92/V.44 Support for Digital Modems
Videoconferencing for the Cisco Multiservice IP-to-IP Gateway Feature
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
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 Record Boundary Preservation for Data Communications Networks
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

Some features are dependent on product model, interface modules (i.e. Line Cards & Port Adapters), and/or require a software feature license. Click here for more information.

Close Window

snmp-server enable traps

To enable all Simple Network Management Protocol (SNMP) notifications (traps or informs) available on your system, use the **snmp-server enable traps** command in global configuration mode. To disable all available SNMP notifications, use the **no** form of this command.

snmp-server enable traps [*notification-type*]

no snmp-server enable traps [*notification-type*]

Syntax Description

notification-type — (Optional) Type of notification (trap or inform) to enable or disable. If no type is specified, all notifications available on your device are enabled or disabled. The notification type can be one of the following keywords:

- **config**—Controls configuration notifications, as defined in the CISCO-CONFIG-MAN-MIB (enterprise 1.3.6.1.4.1.9.9.43.2). The notification type is: (1) ciscoConfigManEvent.
- **ds0-busyout**—Sends notification whenever the busyout of a DS0 interface changes state (Cisco AS5300 platform only). This notification is defined in the CISCO-POP-MGMT-MIB (enterprise 1.3.6.1.4.1.9.10.19.2) and the notification type is:(1) cpmDS0BusyoutNotification
- **ds1-loopback**—Sends notification whenever the DS1 interface goes into loopback mode (Cisco AS5300 platform only). This notification type is defined in the CISCO-POP-MGMT-MIB (enterprise 1.3.6.1.4.1.9.10.19.2) as: (2) cpmDS1LoopbackNotification.
- **entity**—Controls Entity MIB modification notifications. This notification type is defined in the ENTITY-MIB (enterprise 1.3.6.1.2.1.47.2) as: (1) entConfigChange.
- **hsrp**—Controls Hot Standby Routing Protocol (HSRP) notifications, as defined in the CISCO-HSRP-MIB (enterprise 1.3.6.1.4.1.9.9.106.2). The notification type is: (1) cHsrpStateChange.**ipmulticast**—Controls IP Multicast notifications.
- **modem-health**—Controls modem-health notifications.
- **rsvp**—Controls Resource Reservation Protocol (RSVP) flow change notifications.
- **tty**—Controls TCP connection notifications.
- **xgcp**—Sends External Media Gateway Control Protocol (XGCP) notifications. This notification is from the XGCP-MIB-V1SMI.my and the notification is enterprise 1.3.6.1.3.90.2 (1) xgcpUpDownNotification

Note For additional notification types, see the Related Commands table.

Defaults

This command is disabled by default. Most notification types are disabled. However, some notification types cannot be controlled with this command.

If you enter this command with no *notification-type* keyword extenstions, the default is to enable (or diable, if the **no** form is used) all notification types controlled by this command.

Command Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.
12.0(2)T	The **rsvp** keyword was added.
12.0(3)T	The **hsrp** keyword was added.

Usage Guidelines

For additional notification types, see the Related Commands table for this command.

SNMP notifications can be sent as traps or inform requests. This command enables both traps and inform requests for the specified notification types. To specify whether the notifications should be sent as traps or informs, use the **snmp-server host** [**traps** | **informs**] command.

If you do not enter an **snmp-server enable traps** command, no notifications controlled by this command are sent. In order to configure the router to send these SNMP notifications, you must enter at least one **snmp-server enable traps** command. If you enter the command with no keywords, all notification types are enabled. If you enter the command with a keyword, only the notification type related to that keyword is enabled. In order to enable multiple types of notifications, you must issue a separate **snmp-server enable traps** command for each notification type and notification option.

The **snmp-server enable traps** command is used in conjunction with the **snmp-server host** command. Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications. In order to send notifications, you must configure at least one **snmp-server host** command.

Examples

The following example enables the router to send all traps to the host specified by the name myhost.cisco.com, using the community string defined as public:

```
Router(config)# snmp-server enable traps
Router(config)# snmp-server host myhost.cisco.com public
```

The following example enables the router to send Frame Relay and environmental monitor traps to the host myhost.cisco.com using the community string public:

```
Router(config)# snmp-server enable traps frame-relay
Router(config)# snmp-server enable traps envmon temperature
Router(config)# snmp-server host myhost.cisco.com public
```

The following example will not send traps to any host. The BGP traps are enabled for all hosts, but the only traps enabled to be sent to a host are ISDN traps (which are not enabled in this example).

```
Router(config)# snmp-server enable traps bgp
Router(config)# snmp-server host bob public isdn
```

The following example enables the router to send all inform requests to the host at the address myhost.cisco.com, using the community string defined as public:

```
Router(config)# snmp-server enable traps
Router(config)# snmp-server host myhost.cisco.com informs version 2c public
```

The following example sends HSRP MIB traps to the host myhost.cisco.com using the community string public.

```
Router(config)# snmp-server enable traps hsrp
Router(config)# snmp-server host myhost.cisco.com traps version 2c public hsrp
```

Related Commands

Command	Description
snmp-server enable traps atm pvc	Controls (enables or disables) ATM PVC SNMP notifications.
snmp-server enable traps atm pvc extension	Enables the sending of extended ATM permanent virtual circuit (PVC) SNMP notifications.
snmp-server enable traps bgp	Controls (enables or disables) BGP server state change SNMP notifications.
snmp-server enable traps calltracker	Controls (enables or disables) Call Tracker callSetup and callTerminate SNMP notifications.
snmp-server enable traps envmon	Controls (enables or disables) environmental monitor SNMP notifications.
snmp-server enable traps frame-relay	Controls (enables or disables) Frame Relay DLCI link staus change SNMP notifications.
snmp-server enable traps ipsec	Controls (enables or disables) IP Security SNMP notifications.
snmp-server enable traps isakmp	Controls (enables or disables) IPSec Internet Security Association and Key Exchange Protocol (ISAKMP) SNMP notifications.
snmp-server enable traps isdn	Controls (enables or disables) ISDN SNMP notifications.
snmp-server enable traps mpls ldp	Controls (enables or disables) MPLS Label Distribution Protocol (LDP) SNMP notifications.
snmp-server enable traps mpls traffic-eng	Controls (enables or disables) MPLS traffic engineering (TE) tunnel state-change SNMP notifications.
snmp-server enable traps mpls vpn	Controls (enables or disables) MPLS VPN specific SNMP notifications.
snmp-server enable traps repeater	Controls (enables or disables) RFC 1516 Hub notifications.
snmp-server enable traps snmp	Controls (enables or disables) RFC 1157 SNMP notifications.
snmp-server enable traps syslog	Controls (enables or disables) the sending of system logging messages via SNMP.
snmp-server host	Specifies whether you want the SNMP notifications sent as traps or informs, the version of SNMP to use, the security level of the notifications (for SNMPv3), and the destination host (recipient) for the notifications.
snmp-server informs	Specifies inform request options.
snmp-server trap-source	Specifies the interface (and hence the corresponding IP address) that an SNMP trap should originate from.
snmp trap illegal-address	Issues an SNMP trap when a MAC address violation is detected on an Ethernet hub port of a Cisco 2505, Cisco 2507, or Cisco 2516 router.

snmp-server enable traps aaa_server

To enable authentication, authorization, and accounting (AAA) server state-change Simple Network Management Protocol (SNMP) notifications, use the **snmp-server enable traps aaa_server** command in global configuration mode. To disable AAA server state-change SNMP notifications, use the **no** form of this command.

snmp-server enable traps aaa_server

no snmp-server enable traps aaa_server

Syntax Description

This command has no arguments or keywords.

Defaults

SNMP notifications are disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
12.1(3)T	This command was introduced for the Cisco AS5300 and Cisco AS5800.

Usage Guidelines

SNMP notifications can be sent as traps or inform requests. This command enables both traps and inform requests.

This command controls (enables or disables) AAA Server state change (casServerStateChange) notifications. ServerStateChange notifications, when enabled, will be sent when the server moves from an "up" to "dead" state or when a server moves from a "dead" to "up" state.

The Cisco AAA Server State is defined by the casState object in the Cisco AAA Server MIB. The possible values are as follows:

- up(1)—Server is responding to requests.
- dead(2)—Server failed to respond to requests.

A server is marked "dead" if it does not respond after maximum retransmissions. A server is marked "up" again either after a waiting period or if some response is received from it. The initial value of casState is "up(1)" at system startup. This will only transition to "dead(2)" if an attempt to communicate fails.

For a complete description of this notification and additional MIB functions, see the CISCO-AAA-SERVER-MIB.my file, available on Cisco.com at http://www.cisco.com/public/mibs/v2/.

The **snmp-server enable traps aaa_sever** command is used in conjunction with the **snmp-server host** command. Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications. To send SNMP notifications, you must configure at least one **snmp-server host** command.

ANEXO (19 D)

CISCO SYSTEMS

Product Bulletin No. 2239

Standards Supported in Cisco IOS Software Releases 12.3 and 12.2S

Last updated: July 17,2003

This product bulletin lists the major industry standards supported by Cisco IOS® Software Releases 12.3 and 12.2S. It is arranged in reverse chronological order; each section begins with the most recently supported standards.

Note: given the evolving nature of the standardization procedures, this document may not reflect specific drafts, revisions of particular standards, or all the standards that are supported in Cisco IOS Software. Questions of this nature regarding standards not shown below should be directed to the appropriate Cisco IOS Product Manager.

IETF Requests for Comments (RFCs)

The full text for each RFC may be obtained from: http://www.rfc-editor.org/

Table 1 IETF RFC supported in Cisco IOS Software Releases 12.3 and 12.2S

RFC Number	Remarks	RFC Title
RFC 3435	Obsoletes RFC 2705	Media Gateway Control Protocol (MGCP) Version 1.0
RFC 3344	Obsoletes RFC 2002 & RFC 3220	Mobile IP—obsoletes RFC 3220
RFC 3309	Updates RFC 2960	Stream Control Transmission Protocol (SCTP) Checksum Change
RFC 3272		Overview and Principles of Internet Traffic Engineering
RFC 3270		MPLS Support for differentiated Services
RFC 3261	Obsoletes RFC 2543	SIP: Session Initiation Protocol
RFC 3215		LDP State Machine
RFC 3210		Applicability Statements for Extensions to RSVP for LSP Tunnels
RFC 3209		RSVP-TE: Extensions to RSVP for LSP Tunnels
RFC 3115	Obsoletes RFC 3025	Mobile IP Vendor/Organization-Specific Extensions
RFC 3107		Carrying label information in BGP
RFC 3031		Multiprotocol Label Switching Architecture
RFC 3079		Deriving Keys for use with Microsoft Point-to-Point Encryption (MPPE)
RFC 3078		Microsoft Point-To-Point Encryption (MPPE) Protocol
RFC 3064		MGCP CAS Packages

Table 1 IETF RFC supported in Cisco IOS Software Releases 12.3 and 12.2S (Continued)

RFC Number	Remarks	RFC Title
RFC 3063		MPLS Loop Prevention Mechanism
RFC 3057		ISDN Q.921-User Adaptation Layer
RFC 3056		Transmission of IPv6 Domains via IPv4 Clouds (6to4)
RFC 3046		DHCP Relay Agent Information Option
RFC 3038		VCID Notification over ATM link for LDP
RFC 3037		LDP Applicability
RFC 3036		LDP Specification
RFC 3035		MPLS using LDP and ATM VC Switching
RFC 3032		MPLS Lable Stack Encoding
RFC 3031		Multiprotocol Lable Switching Architecture
RFC 3025		Mobile IP Vendor/Organization-Specific Extensions
RFC 3024	Obsoletes RFC 2344	Reverse Tunneling for Mobile IP
RFC 3012		Mobile IPv4 Challenge/Response Extensions
RFC 2977		Mobile IP Authentication, Authorization, and Accounting Requirements
RFC 2961		RSVP Refresh Overhead Reduction Extensions
RFC 2918		Route Refresh Capability for BGP-4
RFC 2915		The Naming Authority Pointer (NAPTR) DNS Resource Record
RFC 2893		Transition Mechanisms for IPv6 Hosts and Routers
RFC 2878		PPP Bridging Control Protocol (BCP)
RFC 2865		Remote Authentication Dial In User Service (RADIUS)
RFC 2858	Obsoletes RFC 2283	Multi-Protocol extensions for BGP4
RFC 2842		Capability Advertisement with BGP-4
RFC 2833		RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals
RFC 2805		Media Gateway Control Protocol Architecture and Requirements
RFC 2796	Updates RFC 1966	BGP Route Reflection
RFC 2794		Mobile IP Network Access Identifier Extension for IPv4
RFC 2782		A DNS RR for specifying the location of services (DNS SRV)
RFC 2766		Network Address Translation - Protocol Translation (NAT-PT)
RFC 2765		Stateless IP/ICMP Translation Algorithm (SIIT)
RFC 2759		Microsoft PPP CHAP Extensions, Version 2
RFC 2749		COPS usage for RSVP

Table 1 IETF RFC supported in Cisco IOS Software Releases 12.3 and 12.2S (Continued)

RFC Number	Remarks	RFC Title
RFC 2747		RSVP Refresh Overhead Reduction Extensions
RFC 2740		OSPF for IPv6
RFC 2705	Obsolete by RFC 3435	Media Gateway Control Protocol v1.0
RFC 2702		Requirements for Traffic Engineering over MPLS
RFC 2698		A Two Rate Three Color Marker
RFC 2697		A Single Rate Three Color Marker (Cisco Class-Based Policier is conformant with the sRTCM)
RFC 2694		DNS Extension to Network Address Translators (DNS_ALG)
RFC 2686		The Multi-Class Extension to Multi-Link PPP
RFC 2684	Obsoletes RFC 1483	Multiprotocol Encapsulation over ATM Adaptation Layer 5
RFC 2661		Layer 2 Tunneling protocol
RFC 2637		Point-to-Point Tunneling Protocol (PPTP)
RFC2616		Hypertext Transfer Protocol—HTTP/1.1
RFC 2598		An Expedited Forwarding PHB
RFC 2597		Assured Forwarding PHB Group
RFC 2590		Transmission of IPv6 Packets over Frame Relay Networks Specification
RFC 2560		Stream Control Transmission Protocol
RFC 2547bis		MPLS-VPNs - Inter-AS and CsC
RFC 2547		BGP/MPLS VPNs
RFC 2545		Use of BGP-4 Multi-Protocol extensions for IPv6 Inter-Domain routing
RFC 2543	Obsolete by RFC 3261	SIP: Session Initiation Protocol
RFC 2529		Transmission of IPv6 over IPv4 Domains without explicit tunnels
RFC 2516		PPP Over Ethernet (PPPoE)
RFC 2509		IP Header Compression over PPP
RFC 2508		Compressing IP/UDP/RTP Headers for Low-Speed Serial Links
RFC 2507		IP Header Compression
RFC 2492		IPv6 over ATM networks
RFC 2475		An Architecture for Differentiated Service
RFC 2474		Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers
RFC 2473		Generic Packet Tunneling in IPv6 specification
RFC 2472		IPv6 over PPP

Table 1 IETF RFC supported in Cisco IOS Software Releases 12.3 and 12.2S (Continued)

RFC Number	Remarks	RFC Title
RFC 2467		Transmission of IPv6 Packets over FDDI Networks
RFC 2464		Transmission of IPv6 Packets over Ethernet Networks
RFC 2463		Internet Control Message Protocol for IPv6 (ICMPv6)
RFC 2462		IPv6 Stateless Address Autoconfiguration
RFC 2461		Neighbor Discovery for IP Version 6 (IPv6)
RFC 2460		Internet Protocol, version 6 (IPv6) specifications
RFC 2453	Obsoletes RFC 1723, 1388	RIP Version 2
RFC 2439		BGP Route Flap Damping
RFC 2433		Microsoft PPP CHAP Extensions
RFC 2427	Obsoletes RFC 1490 & RFC 1294	Multiprotocol Interconnect over Frame Relay
RFC 2409		The Internet Key Exchange (IKE)
RFC 2408		Internet Security Association and Key Management Protocol (ISAKMP)
RFC 2407		The Internet IP Security Domain of Interpretation for ISAKMP
RFC 2406		IP Encapsulation Security Payload (ESP)
RFC 2402		IP Authentication Header
RFC 2401	Obsoletes RFC 1825	Security Architecture for Internet Protocol
RFC 2393		IP Payload Compression Protocol (IPComp)
RFC 2390	Obsoletes RFC 1293	Inverse Address Resolution Protocol
RFC 2374		An Aggregatable Global Unicast Address Format
RFC 2373		IP Version 6 Addressing Architecture
RFC 2370		The OSPF Opaque LSA Option
RFC 2365		(also BCP0023) Administratively Scoped IP Multicast
RFC 2364		PPP over ATM AAL5
RFC 2362	Obsoletes RFC2117	Protocol Independent Multicast-Sparse Mode (PIM-SM)
RFC 2341		Cisco Layer Two Forwarding Protocol (L2F)
RFC 2338		Virtual Router Redundancy Protocol
RFC 2337		Intra-LIS IP Multicast among routers over ATM using Sparse Mode PIM
RFC 2332		NBMA Next Hop Resolution Protocol (NHRP)
RFC 2328	Obsoletes RFC 2178	OSPF Version 2
RFC 2327		SDP: Session Description Protocol

Table 1 IETF RFC supported in Cisco IOS Software Releases 12.3 and 12.2S (Continued)

RFC Number	Remarks	RFC Title
RFC 2326		Real Time Streaming Protocol (RTSP)
RFC 2284		PPP Extensible Authentication Protocol
RFC 2283		Multi-protocol Extension for BGP-4
RFC 2281		Cisco Hot Standby Router Protocol (HSRP)
RFC 2275		View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)
RFC 2274		User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)
RFC 2273		SNMPv3 Applications
RFC 2272		Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)
RFC 2271		An Architecture for Describing SNMP Management Frameworks
RFC 2236		Internet Group Management Protocol, Version 2
RFC 2206		RSVP Management Information Base Using SMIv2
RFC 2205		Resource ReSerVation Protocol (RSVP)
RFC 2166		DLSw + V2
RFC 2131	Obsoletes RFC 1541 & RFC 1531	Dynamic Host Configuration Protocol
RFC 2125		PPP Bandwidth Allocation Protocol (BAP) The PPP Bandwidth Allocation Control Protocol (BACP)
RFC 2127		ISDN Management Information Base Using SMIv2
RFC 2118		Microsoft Point-to-Point Compression (MPPC) Protocol
RFC 2115	Obsoletes RFC 1315	Management Information Base for Frame Relay DTEs
RFC 2091		Triggered Extensions to RIP to Support Demand Circuits
RFC 2080		RIPng
RFC 2037		Entity MIB, Phase I
RFC 2024		DLSw + MIB Enhancements
RFC 2018		TCP Selective Acknowledgment
RFC 2012		SNMP 2C
RFC 2006		The Definitions of Managed Objects for IP Mobility Support Using SMIv2
RFC 2003		IP Encapsulation within IP
RFC 2002		IP Mobility Support

Table 1 IETF RFC supported in Cisco IOS Software Releases 12.3 and 12.2S (Continued)

RFC Number	Remarks	RFC Title
RFC 1997		BGP Communities Attribute
RFC 1994		PPP Challenge Handshake Authentication Protocol
RFC 1990	Obsoletes RFC 1717	PPP Multilink Protocol
RFC 1989	Obsoletes RFC 1333	PPP Link Quality Monitoring
RFC 1981		Path MTU Discovery for IP version 6
RFC 1974		LZS STAC Compression
RFC 1973		PPP in Frame Relay
RFC 1967		PPP LZS-DCP Compression Protocol (LZS-DCP)
RFC 1966		BGP Route Reflection
RFC 1965		Autonomous System Confederation for BGP
RFC 1962		The PPP Compression Control Protocol (CCP)
RFC 1918		Address Allocation for Private Internets
RFC 1907	Obsoletes RFC 1450	Management Information Base for Version 2 of the Simple Network Management Protocol (SNMPv2)
RFC 1906	Obsoletes RFC 1449	Transport Mappings for Version 2 of the Simple Network Management Protocol (SNMPv2)
RFC 1905	Obsoletes RFC 1448	Protocol Operations for Version 2 of the Simple Network Management Protocol (SNMPv2)
RFC 1904	Obsoletes RFC 1444	Conformance Statements for Version 2 of the Simple Network Management Protocol (SNMPv2)
RFC 1889		RTP: A Transport for Real-Time Applications
RFC 1886		DNS extensions to support IPv6
RFC 1877		PPP Internet Protocol Control Protocol Extensions for Name Server Addresses
RFC 1829		The ESP DES-CBC Transform
RFC 1828		IP Authentication Using Keyed MD5
RFC 1827		IP Encapsulating Security Payload (ESP)
RFC 1826		IP Authentication Header
RFC 1812		Requirements for IP Version 4 Routers
RFC 1795	Makes RFC 1434 obsolete	Data Link Switching (DLSw): Switch-to-Switch Protocol AIW DLSw RIG: DLSw Closed Pages, DLSw Version 1.0
RFC 1793		Extending OSPF to Support Demand Circuits
RFC 1771	Supersedes RFC 1654	A Border Gateway Protocol (BGP-4)

Table 1 IETF RFC supported in Cisco IOS Software Releases 12.3 and 12.2S (Continued)

RFC Number	Remarks	RFC Title
RFC 1765		OSPF Database Overflow
RFC 1757	Supersedes RFC 1271	Remote Network Monitoring (RMON) Management Information Base
RFC 1755		ATM Signaling Support for IP over ATM
RFC 1745		BGP4/IDRP for IP—OSPF Interaction
RFC 1724		RIP Version 2 MIB Extension
RFC 1723		RIP Version 2 Carrying Additional Information
RFC 1722		RIP Version 2 Protocol Applicability Statement
RFC 1717	Obsolete by RFC 1990	The PPP Multilink Protocol (MP)
RFC 1706	Obsoletes RFC 1637, 1348	DNS NSAP Resource Records
RFC 1701		Generic Route Encapsulation (GRE)
RFC 1702		Generic Routing Encapsulation over IPv4 networks
RFC 1695		Definitions of Management Objects for ATM Management Version 8.0 Using SMIv2
RFC 1663		PPP Reliable Transmission
RFC 1662	bit-oriented/async only - obsoletes RFC 1549	PPP in HDLC-like Framing
RFC 1661	Obsoletes RFC 1548	PPP (Point-to-Point Protocol)
RFC 1657		Definitions of Managed Objects for Version 4 of the Border Gateway Protocol (BGP-4) Using SMIv2
RFC 1647		TN3270 Enhancements
RFC 1646	LU Name Selection only	TN3270 Extensions for LUname and Printer Selection
RFC 1638		PPP Bridging Control Protocol (BCP)
RFC 1634	Supersedes 1362 and 1551	Novell Routing over Various WAN Media (IPXWAN)
RFC 1631		The IP Network Address Translator (NAT)
RFC 1619		PPP over SONET
RFC 1618		PPP over ISDN
RFC 1613		X.25 over TCP, XOT
RFC 1595		Definitions of Managed Objects for the SONET/SDH Interface Type
RFC 1593		SNA APPN Node MIB
RFC 1587		The OSPF NSSA Option

Table 1 IETF RFC supported in Cisco IOS Software Releases 12.3 and 12.2S (Continued)

RFC Number	Remarks	RFC Title
RFC 1583	Supersedes 1247	OSPF Version 2
RFC 1577		Classical IP and ARP over ATM
RFC 1576		TN3270 Current Practices
RFC 1573		Evolution of the Interfaces Group of MIB-II
RFC 1570		PPP LCP Extensions
RFC 1559		DECnet Phase IV MIB Extensions
RFC 1553		Compressing IPX Headers over WAN Media (CIPX)
RFC 1552		The PPP Internetwork Packet Exchange Control Protocol (IPXCP)
RFC 1549	Obsolete by RFC 1662	PPP in HDLC Framing
RFC 1548	Obsolete by RFC 1661	The Point-to-Point Protocol (PPP)
RFC 1542	BOOTP relay agent	Clarifications and Extensions for the Bootstrap Protocol
RFC 1534		Interoperation between DHCP and BOOTP
RFC 1519		Classless Inter-Domain Routing (CIDR): an Address Assignment and Aggregation Strategy
RFC 1512	Updates RFC 1285	FDDI Management Information Base
RFC 1510		The Kerberos Network Authentication Service (V5)
RFC 1497		BOOTP Vendor Extensions
RFC 1493	Obsoletes RFC 1286	Definitions of Managed Objects for Bridges
RFC 1492		Access Control Protocol or TACACS
RFC 1469		IP Multicast over Token Ring LANs
RFC 1450	Obsolete by RFC1907	MIB for SNMP Version 2
RFC 1449	Obsolete by RFC1906	Transport Mappings for Version 2 of the Simple Network Management Protocol (SNMPv2)
RFC 1448	Obsolete by RFC1905	Protocol Operations for Version 2 of the Simple Network Management Protocol (SNMPv2)
RFC 1447		Party MIB for Version 2 of the Simple Network Management Protocol (SNMPv2)
RFC 1445		Administrative Model for Version 2 of the Simple Network Management Protocol (SNMPv2)
RFC 1444	Obsolete by RFC1904	Conformance Statements for Version 2 of the Simple Network Management Protocol (SNMPv2)
RFC 1413		Identification Protocol
RFC 1407	Obsoletes RFC 1233	Definitions of Managed Objects for the DS3/E3 Interface Type

Table 1 IETF RFC supported in Cisco IOS Software Releases 12.3 and 12.2S (Continued)

RFC Number	Remarks	RFC Title
RFC 1406		Definitions of Managed Objects for the DS1 and E1 Interface Types
RFC 1403		BGP OSPF Interaction
RFC 1398		Definitions of Managed Objects for Ethernet-Like Interface Types
RFC 1395		BOOTP Extensions
RFC 1393		Traceroute Using an IP Option
RFC 1390		Transmission of IP and ARP over FDDI Networks
RFC 1382		SNMP MIB Extension for X.25 Packet Layer
RFC 1381		SNMP MIB Extension for X.25 LAPB
RFC 1378	Partial support	PPP AppleTalk Control Protocol (ATCP)
RFC 1377		PPP OSI Network Layer Control Protocol (OSINLCP)
RFC 1376		PPP DECnet Phase IV Control Protocol (DNCP)
RFC 1370		Applicability Statement for OSPF
RFC 1362		Novell IPX Over Various WAN Media (IPXWAN)
RFC 1356		Multiprotocol Interconnect on X.25 and ISDN in the Packet Mode
RFC 1350		TFTP Version 2
RFC 1349		Type of Service in the Internet Protocol Suite
RFC 1334		PPP Authentication Protocols
RFC 1333	Obsolete by RFC 1989	PPP Link Quality Monitoring
RFC 1332		PPP Internet Protocol Control Protocol (IPCP)
RFC 1331	Replaced by RFC 1548	PPP for the Transmission of Multiprotocol Datagrams over Point-to-Point Links
RFC 1323		TCP Extensions for High Performance
RFC 1321		The MD5 Message-Digest Algorithm
RFC 1317		Definitions of Managed Objects for RS-232-like Hardware Devices
RFC1315		Management Information Base for Frame Relay DTEs
RFC 1305		Network Time Protocol (NTP) Version 3
RFC 1286		Definitions of Managed Objects for Bridges
RFC 1268		Application of BGP in the Internet
RFC 1256		ICMP Router Discovery Messages
RFC 1253		MIB for OSPF Version 2
RFC 1243		AppleTalk Management Information Base

Table 1 IETF RFC supported in Cisco IOS Software Releases 12.3 and 12.2S (Continued)

RFC Number	Remarks	RFC Title
RFC 1236		IP to X.121 Address Mapping for DDN
RFC 1234		Tunneling IPX Traffic through IP Networks
RFC 1231	Partial support	IEEE 802.5 Token Ring MIB
RFC 1220		Point-to-Point Protocol (PPP) Extensions for Bridging
RFC 1215		Convention for Defining Traps for Use with SNMP
RFC 1213		Management Information Base for Network Management of TCP/IP-Based Internets: MIB-II
RFC 1212		Concise MIB Definitions.
RFC 1209		Transmission of IP Datagrams over SMDS Service
RFC 1196		Finger User Information Protocol
RFC 1195		Use of OSI IS-IS for Routing in TCP/IP in Dual Environments
RFC 1191		Path MTU Discovery
RFC 1172		PPP Initial Configuration Options
RFC 1157		Simple Network Management Protocol (SNMP)
RFC 1144		Compressing TCP/IP Headers for Low-Speed Serial Links
RFC 1144		TCP/IP Header Compression (Van Jacobson Method)
RFC 1141		Incremental Updating of the Internet Checksum
RFC 1139		Echo Function for ISO 8473 (PING)
RFC 1136		Administrative Domains and Routing Domains: A Model for Routing in the Internet
RFC 1122		Requirements for Internet Hosts—Communication Layers
RFC 1112		Host Extensions for IP Multicasting
RFC 1108	DCA Draft	IP Security Option (IPSO)
RFC 1101		DNS Encoding of Network Names and Other Types
RFC 1091		Telnet Terminal-Type Option
RFC 1084		BOOTP Extensions
RFC 1080		Telnet Remote Flow Control Option
RFC 1079		Telnet Terminal Speed Option
RFC 1075	Interoperate	Distance Vector Multicast Routing Protocol
RFC 1070		Use of the Internet as a Subnetwork for Experimentation with the OSI Network Layer

Table 1 IETF RFC supported in Cisco IOS Software Releases 12.3 and 12.2S (Continued)

RFC Number	Remarks	RFC Title
RFC 1069		Guidelines for the Use of Internet-IP Addresses in the ISO Connectionless-Mode Network Protocol
RFC 1058		Routing Information Protocol (RIP)
RFC 1055		Standard for the Transmission of IP Datagrams over Serial Lines: SLIP
RFC 1042		Standard for the Transmission of IP Datagrams over IEEE 802 Networks
RFC 1035		Domain Names—Implementation and Specification
RFC 1034		Domain Names—Concepts and Facilities
RFC 1027		Using ARP to Implement Transparent Subnet Gateways (Proxy ARP)
RFC 995	Replaced by ISO 9542	ES-to-IS Routing Exchange Protocol for Use in Conjunction with ISO 8473
RFC 994	Replaced by ISO 8473	Protocol for Providing the Connectionless-Mode Network Service
RFC 982		Guidelines for the Specification of the Top of the Structure of the Domain Specific Part (DSP) of the ISO standard NSAP address
RFC 974		Mail Routing and The Domain System
RFC 951		Bootstrap Protocol (BootP)
RFC 950		Internet standard Subnetting Procedure
RFC 925		Multi-LAN Address Resolution (PROXY ARP)
RFC 922		Broadcasting Internet Datagrams in the Presence of Subnets (IP_BROAD)
RFC 919		Broadcasting Internet datagrams
RFC 906		Bootstrap Loading Using TFTP
RFC 904		Exterior Gateway Protocol (EGP) Formal Specification
RFC 903		Reverse Address Resolution Protocol (RARP)
RFC 896		Congestion Control in TCP/IP Internetworks
RFC 895		Standard for the Transmission of IP Datagrams over Experimental Ethernet Networks
RFC 894		Standard for the Transmission of IP Datagrams over Ethernet
RFC 891		Hello Protocol
RFC 879		The TCP Maximum Segment Size and Related Topics
RFC 877		Standard for the Transmission of IP Datagrams over Public Data Networks
RFC 874		Telnet Protocol Specification
RFC 863		Discard Service (TCP Discard)

Table 1 IETF RFC supported in Cisco IOS Software Releases 12.3 and 12.2S (Continued)

RFC Number	Remarks	RFC Title
RFC 862		Echo Service (TCP Echo)
RFC 860		Telnet Timing Mark Option
RFC 858		Telnet Suppress Go Ahead Option
RFC 857		Telnet Echo Option
RFC 856		Telnet Binary Transmission
RFC 855		Telnet Option Specification
RFC 854	MIL STD 1782	Telnet Protocol Specification
RFC 827		Exterior Gateway Protocol (EGP)
RFC 826		Address Resolution Protocol (ARP)
RFC 815		IP Datagram Reassembly Algorithms
RFC 813		Window and Acknowledgment Strategy in TCP/IP
RFC 793	MIL STD 1778	Transmission Control Protocol (TCP)
RFC 792		Internet Control Message Protocol (ICMP)
RFC 791	MIL STD 1777	Internetwork Protocol (IP)
RFC 783		Trivial File Transfer Protocol (TFTP) (Version 2)
RFC 779		Telnet Send-Location Option
RFC 768		User Datagram Protocol (UDP)

Drafts

L2TPv3 - draft-ietf-l2tpext-l2tp-base-03
Routing IPv6 with IS-IS -draft-ietf-isis-ipv6
Multi-Topology Routing in IS-IS - draft-ietf-isis-wg-multi-topology
Connecting IPv6 Islands across IPv4 Clouds with BGP - draft-ietf-ngtrans-bgp-tunnel
Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) - draft-ietf-ngtrans-isatap
IP MIB - draft-ietf-ipv6-rfc2011-update
IP Forwarding Table MIB - draft-ietf-ipv6-rfc2096-update
LSP Ping - draft-ietf-mpls-lsp-ping-01
MPLS Fast ReRoute - draft-ietf-mpls-rsvp-lsp-fastreroute-02
AToM - draft-martini-l2circuit-trans-mpls-10.
draft-martini-l2circuit-encap-mpls-04
Nat-traversal IPSec:
draft-ietf-ipsec-nat-t-ike-03
draft-ietf-ipsec-nat-t-ike-02
draft-ietf-ipsec-udp-encaps-03
A Border Gateway Protocol 4 (BGP-4) - draft-ietf-idr-bgp4-20
BGP Extended Communities Attribute - draft-ietf-idr-bgp-ext-communities-05

Graceful Restart Mechanism for BGP - draft-ietf-idr-restart-06

The AES Cipher Algorithm and Its Use With IPsec - draft-ietf-ipsec-ciph-aes-cbc-04
SIP-Specific Event Notification - draft-ietf-sip-events-01
ISUP to SIP Mapping draft - draft-ietf-sip-isup-03
A Media Resource Control Protocol Developed by Cisco, Nuance, and Speechworks - draft-shanmugham-mrcp-04

IEEE Standards

The full text for each standard may be obtained from: http://www.ieee.com

Table 2 IEEE standards supported in Cisco IOS Software Release 12.3 and 12.2S

802.1	LAN/MAN bridging and management
802.1Q	Virtual LANs
802.3	CSMA/CD (Ethernet)
802.5	Token ring access method and physical layer specification

ATM Forum Standards

The full text for each standard may be obtained from: http://www.atmforum.com

Table 3 IEEE standards supported in Cisco IOS Software Releases 12.3 and 12.2S Software

ILMI (Integrated Local Management Interface)	ILMI 4.0 (af-ilmi-0065.000)
User-to-Network Interface	UNI 3.0 and 3.1 (af-uni-0010.002)
LAN Emulation (Version 2)	Ethernet and Token Ring (af-lane-0021.000)
Multiprotocol over ATM (Version 1)	MPOA (af-mpoa-0087.000)
Private Network-Network Interface	PNNI Version 1 (af-pnni-0055.000)

Frame Relay Forum Standards

The full text for each standard may be obtained from: http://www.frforum.com

Frame Relay Forum standards supported in Cisco IOS Software:

- User-to-Network (UNI) Implementation Agreement—FRF.1.2
- Frame Relay Network-to-Network (NNI) Implementation Agreement Version 2.1—FRF.2.1
- Multiprotocol Encapsulation Implementation Agreement (MEI)—FRF.3.2
- SVC User-to-Network Interface (UNI) Implementation Agreement—FRF.4.1
- Frame Relay/ATM Network Internetworking Implementation Agreement—FRF.5
- Frame Relay/ATM PVC Service Internetworking Implementation Agreement—FRF.8.1
- Data Compression over Frame Relay Implementation Agreement —FRF.9
- Voice over Frame Relay Implementation Agreement—FRF.11

- Frame Relay Fragmentation Implementation Agreement—FRF.12
- Frame Relay Forum Implementation Agreement FRF.11 for Data Compression
- Frame Relay Forum Implementation Agreement FRF.16 for Multilink Frame Relay

ITU-T/CCITT Standards

More information for each standard may be obtained from: http://www.itu.int/

- X.3—ITU-T/CCITT 1993 mandatory
- X.25—ITU-T/CCITT 1993
- X.28—ITU-T/CCITT 1993
- X.29—ITU-T/CCITT 1993
- X.31—X.25 on ISDN
- X.121—Addressing scheme
- ITU-T H.323 Packet-based multimedia communications systems
- ITU-T T.37 Procedures for the transfer of facsimile data via store-and-forward on the Internet
- ITU-T T.38, Procedures for real-time Group 3 facsimile communication over IP networks
- ITU-T T.38, Procedures for real-time Group 3 facsimile communication over IP networks, Amendment 1
- ITU-T, Revised Annex B of Recommendation T.38

ITU Standards for Voice CODECs:

- g711alaw G.711 A Law 64000 bps
- g711ulaw G.711 u Law 64000 bps
- g723ar53 G.723.1 ANNEX-A 5300 bps
- g723ar63 G.723.1 ANNEX-A 6300 bps
- g723r53 G.723.1 5300 bps
- g723r63 G.723.1 6300 bps
- g726r16 G.726 16000 bps
- g726r24 G.726 24000 bps
- g726r32 G.726 32000 bps
- g728 G.728 16000 bps
- g729br8 G.729 ANNEX-B 8000 bps
- g729r8 G.729 8000 bps
- gsmefr GSMEFR 12200 bps
- gsmfr GSMFR 13200 bps

ITU-T Q.931 (and related standards)—ISDN user-network interface layer 3 specification for basic call control

Additional Standards

PacketCable. PSTN Gateway Call Signaling Protocol Specification , Pkt-SP-TGCP-D02-991028, Dec 1, 1999

PacketCable. Network-Based Call Signaling Protocol Specification, PKT-SP-EC-MGCP-I02-991201, Dec 1, 1999

PacketCable PSTN Gateway Call Signaling Protocol Specification, Pkt-SP-TGCP-101-991024, October 24, 1999.

PacketCable Network-Based Call Signaling Protocol Specification, Pkt-SP-EC-MGCP-102-991024, October 24, 1999.

Telecordia SM 1.5 (Simple Gateway Control Protocol)

VoiceXML Version 2.0, W3C Working Draft October 23, 2001—Working draft that defines VoiceXML:—http://www.w3.org/Voice/

ECMA-262, ECMAScript Language Specification, 3rd edition August 1998—Defines the ECMAScript scripting language—http://www.ecma-international.org/

ECMA (series of standards for QSIG)—http://www.ecma-international.org/

QSIG Standards supported (with certain exceptions):

ECMA 141, 142, 143(ETSI300-172), 165(ETSI239), Q.SIG v1 & v2

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 • Scorland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Configuring TCP Intercept (Preventing Denial-of-Service Attacks)

This chapter describes how to configure your router to protect TCP servers from TCP SYN-flooding attacks, a type of denial-of-service attack. This is accomplished by configuring the Cisco IOS feature known as TCP Intercept.

For a complete description of TCP Intercept commands, refer to the "TCP Intercept Commands" chapter of 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 chapter "Identifying Supported Platforms" section in the "Using Cisco IOS Software."

In This Chapter

This chapter has the following sections:

About TCP Intercept

The TCP intercept feature implements software to protect TCP servers from TCP SYN-flooding attacks, which are a type of denial-of-service attack.

A SYN-flooding attack occurs when a hacker floods a server with a barrage of requests for connection. Because these messages have unreachable return addresses, the connections cannot be established. The resulting volume of unresolved open connections eventually overwhelms the server and can cause it to deny service to valid requests, thereby preventing legitimate users from connecting to a web site, accessing e-mail, using FTP service, and so on.

The TCP intercept feature helps prevent SYN-flooding attacks by intercepting and validating TCP connection requests. In intercept mode, the TCP intercept software intercepts TCP synchronization (SYN) packets from clients to servers that match an extended access list. The software establishes a connection with the client on behalf of the destination server, and if successful, establishes the

connection with the server on behalf of the client and knits the two half-connections together transparently. Thus, connection attempts from unreachable hosts will never reach the server. The software continues to intercept and forward packets throughout the duration of the connection.

In the case of illegitimate requests, the software's aggressive timeouts on half-open connections and its thresholds on TCP connection requests protect destination servers while still allowing valid requests.

When establishing your security policy using TCP intercept, you can choose to intercept all requests or only those coming from specific networks or destined for specific servers. You can also configure the connection rate and threshold of outstanding connections.

You can choose to operate TCP intercept in watch mode, as opposed to intercept mode. In watch mode, the software passively watches the connection requests flowing through the router. If a connection fails to get established in a configurable interval, the software intervenes and terminates the connection attempt.

TCP options that are negotiated on handshake (such as RFC 1323 on window scaling) will not be negotiated because the TCP intercept software does not know what the server can do or will negotiate.

TCP Intercept Configuration Task List

To configure TCP intercept, perform the tasks in the following sections. The first task is required; the rest are optional.

- Enabling TCP Intercept (Required)
- Setting the TCP Intercept Mode (Optional)
- Setting the TCP Intercept Drop Mode (Optional)
- Changing the TCP Intercept Timers (Optional)
- Changing the TCP Intercept Aggressive Thresholds (Optional)
- Monitoring and Maintaining TCP Intercept (Optional)

For TCP intercept configuration examples using the commands in this chapter, refer to the "TCP Intercept Configuration Example" section at the end of this chapter.

Enabling TCP Intercept

To enable TCP intercept, use the following commands in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# access-list access-list-number {deny | permit} tcp any destination destination-wildcard`	Defines an IP extended access list.
Step 2	`Router(config)# ip tcp intercept list access-list-number`	Enables TCP intercept.

You can define an access list to intercept all requests or only those coming from specific networks or destined for specific servers. Typically the access list will define the source as **any** and define specific destination networks or servers. That is, you do not attempt to filter on the source addresses because you do not necessarily know who to intercept packets from. You identify the destination in order to protect destination servers.

If no access list match is found, the router allows the request to pass with no further action.

Setting the TCP Intercept Mode

The TCP intercept can operate in either active intercept mode or passive watch mode. The default is intercept mode.

In intercept mode, the software actively intercepts each incoming connection request (SYN) and responds on behalf of the server with an SYN-ACK, then waits for an ACK from the client. When that ACK is received, the original SYN is sent to the server and the software performs a three-way handshake with the server. When this is complete, the two half-connections are joined.

In watch mode, connection requests are allowed to pass through the router to the server but are watched until they become established. If they fail to become established within 30 seconds (configurable with the **ip tcp intercept watch-timeout** command), the software sends a Reset to the server to clear up its state.

To set the TCP intercept mode, use the following command in global configuration mode:

Command	Purpose
`Router(config)# ip tcp intercept mode {intercept | watch}`	Sets the TCP intercept mode.

Setting the TCP Intercept Drop Mode

When under attack, the TCP intercept feature becomes more aggressive in its protective behavior. If the number of incomplete connections exceeds 1100 or the number of connections arriving in the last one minute exceeds 1100, each new arriving connection causes the oldest partial connection to be deleted. Also, the initial retransmission timeout is reduced by half to 0.5 seconds (so the total time trying to establish a connection is cut in half).

By default, the software drops the oldest partial connection. Alternatively, you can configure the software to drop a random connection. To set the drop mode, use the following command in global configuration mode:

Command	Purpose
`Router(config)# ip tcp intercept drop-mode {oldest | random}`	Sets the drop mode.

Changing the TCP Intercept Timers

By default, the software waits for 30 seconds for a watched connection to reach established state before sending a Reset to the server. To change this value, use the following command in global configuration mode:

Command	Purpose
`Router(config)# ip tcp intercept watch-timeout` *seconds*	Changes the time allowed to reach established state.

By default, the software waits for 5 seconds from receipt of a reset or FIN-exchange before it ceases to manage the connection. To change this value, use the following command in global configuration mode:

Command	Purpose
`Router(config)# ip tcp intercept finrst-timeout` *seconds*	Changes the time between receipt of a reset or FIN-exchange and dropping the connection.

By default, the software still manages a connection for 24 hours after no activity. To change this value, use the following command in global configuration mode:

Command	Purpose
`Router(config)# ip tcp intercept connection-timeout` *seconds*	Changes the time the software will manage a connection after no activity.

Changing the TCP Intercept Aggressive Thresholds

Two factors determine when aggressive behavior begins and ends: total incomplete connections and connection requests during the last one-minute sample period. Both thresholds have default values that can be redefined.

When a threshold is exceeded, the TCP intercept assumes the server is under attack and goes into aggressive mode. When in aggressive mode, the following occurs:

- Each new arriving connection causes the oldest partial connection to be deleted. (You can change to a random drop mode.)
- The initial retransmission timeout is reduced by half to 0.5 seconds, and so the total time trying to establish the connection is cut in half. (When not in aggressive mode, the code does exponential back-off on its retransmissions of SYN segments. The initial retransmission timeout is 1 second. The subsequent timeouts are 2 seconds, 4 seconds, 8 seconds, and 16 seconds. The code retransmits 4 times before giving up, so it gives up after 31 seconds of no acknowledgment.)
- If in watch mode, the watch timeout is reduced by half. (If the default is in place, the watch timeout becomes 15 seconds.)

The drop strategy can be changed from the oldest connection to a random connection with the **ip tcp intercept drop-mode** command.

Note The two factors that determine aggressive behavior are related and work together. When *either* of the **high** values is exceeded, aggressive behavior begins. When *both* quantities fall below the **low** value, aggressive behavior ends.

You can change the threshold for triggering aggressive mode based on the total number of incomplete connections. The default values for **low** and **high** are 900 and 1100 incomplete connections, respectively. To change these values, use the following commands in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# ip tcp intercept max-incomplete low` *number*	Sets the threshold for stopping aggressive mode.
Step 2	`Router(config)# ip tcp intercept max-incomplete high` *number*	Sets the threshold for triggering aggressive mode.

You can also change the threshold for triggering aggressive mode based on the number of connection requests received in the last 1-minute sample period. The default values for **low** and **high** are 900 and 1100 connection requests, respectively. To change these values, use the following commands in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# ip tcp intercept one-minute low` *number*	Sets the threshold for stopping aggressive mode.
Step 2	`Router(config)# ip tcp intercept one-minute high` *number*	Sets the threshold for triggering aggressive mode.

Monitoring and Maintaining TCP Intercept

To display TCP intercept information, use either of the following commands in EXEC mode:

Command	Purpose
`Router# show tcp intercept connections`	Displays incomplete connections and established connections.
`Router# show tcp intercept statistics`	Displays TCP intercept statistics.

TCP Intercept Configuration Example

The following configuration defines extended IP access list 101, causing the software to intercept packets for all TCP servers on the 192.168.1.0/24 subnet:

```
ip tcp intercept list 101
!
access-list 101 permit tcp any 192.168.1.0 0.0.0.255
```

ANEXO (19F)

Cisco – Software Installation and Upgrade Procedure

Table of Contents

Software Installation and Upgrade Procedure

for the 1000, 1400, 1600–R, 1700, 2600, 3600, 3700, 4000, 4500, 4700, AS5300, and the MC3810

Introduction

This document explains the procedure for upgrading a Cisco IOS® software image on Access router platforms. The examples provided from the 2600 and 3600 Series Routers also apply to the list of router platforms mentioned below. The Cisco IOS software file names may vary depending on the Cisco IOS software version, feature set, and platform.The following Cisco series routers are addressed in this document:

- Cisco 1000 Series Routers
- Cisco 1400Series Routers
- Cisco 1600–R Series Routers
- Cisco 1700 Series Routers
- Cisco 2600 Series Routers
- Cisco 3600 Series Routers
- Cisco 3700 Series Routers
- Cisco 4000 Series Routers
- Cisco 4700 Series Routers
- Cisco AS5300 Series Routers
- Cisco MC3810 Series Routers

Note: To use the troubleshooting tools described in this document, you must be a user and you must be .

Before You Begin

Conventions

For more information on document conventions, see the Cisco Technical Tips Conventions.

Prerequisites

Step 1: Install a TFTP Server

A Trival File Transfer Protocol (TFTP) server or a Remote Copy Protocol (RCP) server application must be installed on a TCP/IP–ready workstation or PC. Once the application is installed, a minimal level of configuration must be performed.

1. The TFTP application must be configured to operate as a TFTP *server* as opposed to a TFTP *client*.
2. The outbound file directory must be specified. This is the directory in which the Cisco IOS software images are stored (see step 2 below). Most TFTP applications provide a set–up routine to assist in these configuration tasks.

   Note: A number of TFTP or RCP applications are available from independent software vendors or as shareware from public sources on the World Wide Web.

Step 2: Select a Cisco IOS Software Image

Verify that the Cisco IOS Software image that you download supports both your hardware and the required software features. You can find this information using the Cisco Software Advisor (registered customers only) . Make sure that your router has enough Dynamic RAM (DRAM) and Flash for the Cisco IOS software image prior to downloading the software version you have selected. You can find the minimum recommended DRAM and Flash requirements in the release notes for each specific Cisco IOS software version, as well as in the Cisco IOS Upgrade Planner (registered customers only) .

For additional information on how to select the right software version and feature set, see How to Choose a Cisco IOS Software Release.

Step 3: Download the Cisco IOS Software Image

Download the Cisco IOS Software image into your workstation or PC from the Cisco IOS Upgrade Planner (registered customers only) .

Should you experience any problems while using TFTP to upgrade your router, see Common Problems in Installing Images Using TFTP.

Components Used

The information in this document is based on Cisco IOS Software Release 12.0 or later.

The information presented in this document was created from devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If you are working in a live network, ensure that you understand the potential impact of any command before using it.

Upgrade Procedure for Routers with Internal Flash (for example, 2600 Series Routers)

The upgrade procedure involves three main steps:

1. Establish a console session to the router
2. Verify that the TFTP server has IP connectivity to the router
3. Copy the new image into the Flash memory of the 2600 Series Router through the TFTP server

Establish a console session to the router

Even if it is possible to connect to the router through a telnet session, it is strongly recommended to be directly connected to the router using the console port. The reason is that if something goes wrong during the upgrade, it might be necessary to be physically located next to the router to power–cycle it. Moreover, the telnet connection will be lost while the router is rebooting during the upgrade procedure.

A rolled cable (usually a flat black cable) is used to connect, and connects the console port of the router to one of the COM ports of the PC.

Once the PC is connected to the console port of the router, you need to open hyperterminal on the PC, and use the following settings:

```
Speed 9600 bits per second
8 databits
0 parity bits
1 stop bit
No Flow Control
```

Note: If you are getting any garbage characters in the hyperterminal session, this means that you have not set the hyperterminal properties properly, or the configuration register of the router is set to a non–standard value for which the console connection speed is higher than 9600 bps. Check the value of the configuration register using the **show version** command (shown in the last line of the output) and ensure it is set to 0x2102 or 0x102. It is necessary to reload the router for a configuration register change to take effect. Once you are sure the console speed is set to 9600 bps on the router side, you should check the hyperterminal properties as above . For more information on setting the hyperterminal properties, see Applying Correct Terminal Emulator Settings for Console Connections.

Booting Problems

Once you are connected to the console port of the router, you might notice that the router is either in ROMmon or Boot mode. These two modes are used for recovery and/or diagnostic procedures. If you do not see the usual router prompt, you should follow the recommendations below to proceed with the upgrade procedure installation.

- Router boots in rommon mode, and the following message appears when you issue **dir flash:** command.

```
rommon 1 > dir flash:
device does not contain a valid magic number
dir: cannot open device "flash:"
rommon 2 >
```

  When you see the above error message, it means the Flash is empty or the filesystem is corrupted. See Xmodem console download procedure using ROMmon.
- Router boots in boot mode, with the following messages on the console:

```
router(boot)>
```

```
device does not contain a valid magic number
boot: cannot open "flash:"
boot: cannot determine first file name on device "flash:"
```

When you get the above error messages on the console output, it means the Flash is empty or the file system is corrupted. Copy a valid image on the Flash by following the procedures provided in this document.

Verify that the TFTP server has IP connectivity to the router

The TFTP server must have a network connection to the router, and must be able to ping the IP address of the router targeted for a TFTP software upgrade. To achieve this, the router interface and the TFTP server must have:

- an IP address in the same range, or
- a default gateway configured.

To verify this, check the IP address of the TFTP server. See Determining IP Addresses for more details.

Copy the new image into the Flash memory of the router through the TFTP server

Follow these steps:

1. Now that you have IP connectivity and can ping between the computer acting as a TFTP server and the router, copy the Cisco IOS software image into the Flash.

   Note: Before copying, make sure you have started the TFTP server software on your PC and that you have the filename mentioned in the TFTP server root directory. We recommend that you keep a backup of the router/access server configuration before upgrading. The upgrade itself does not affect the configuration (which is stored in nonvolatile RAM (NVRAM). However, this might happen if the steps are not followed properly.

   For RCP applications, substitute RCP for every occurrence of TFTP. For example, use the **copy rcp flash** command instead of the **copy tftp flash** command.

   ```
   2600> enable
   Password:xxxxx
   2600#
   2600# copy tftp flash
   ```

   If necessary, you can copy an image from one device to another.
2. Specify the IP address of the TFTP server.

   When prompted, enter the IP address of the TFTP server as in the following example:

   ```
   Address or name of remote host []? 10.10.10.2
   ```

3. Specify the filename of the new Cisco IOS software image.

   When prompted, enter the filename of the Cisco IOS software image to be installed, as in the following example:

   ```
   Source filename []? c2600-i-mz.121-14.bin
   ```

Note: The filename is case sensitive, so be sure to enter it correctly.

4. Specify the destination filename.

   This is the name the new software image will have when it is loaded onto the router. The image can be named anything, but common practice is to enter the same image filename.

```
Destination filename []? c2600-i-mz.121-14.bin
```

Note: If you see the below error message:

```
%Error copying tftp://10.10.10.2/c2600-i-mz.121-14.bin
(Not enough space on device)
```

Note: This indicates that there is not enough room available in Flash to copy the image. You need to erase a file(s) before copying the new image from the TFTP server.

5. Upgrade the new image from a TFTP server

```
2610#copy tftp flash
Address or name of remote host []? 10.10.10.2
Source filename []? c2600-i-mz.121-14.bin
Destination filename [c2600-i-mz.121-14.bin]?y
Accessing tftp://10.10.10.2/c2600-i-mz.121-14.bin...
Erase flash: before copying? [confirm]y
!---If there is not enough


!--- memory available, erase the Flash

Erasing the flash filesystem will remove all files! Continue? [confirm]y
Erasing device... eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee
eeeeeeeeee ...erased
Erase of flash: complete
Loading c2600-i-mz.121-14.bin from 10.10.10.2 (via Ethernet0/0): !!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 4501480/9001984 bytes]

Verifying checksum...  OK (0xAC8A)
4501480 bytes copied in 56.88 secs (80383 bytes/sec)
```

The copying process takes several minutes; the time differs from network to network. During the copy process, messages are displayed to indicate which file has been accessed.

The exclamation point "!" indicates that the copy process is taking place. Each exclamation point indicates that ten packets have been transferred successfully. A checksum verification of the image occurs after the image is written to Flash memory.

Information about troubleshooting software transfer problems is available at Common Problems in Installing Images Using TFTP or an RCP Server.

6. After you have upgraded the Flash, you need to reload the router using the **reload** command.

Before you reload the router, you need to check two things:

- The value of the config-register – You can check this using the **show version** command. The value is shown in the last line of the **show version** output. It should be set to 0x2102.

```
2610#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
2610(config)#config-register 0x2102
2610(config)#^Z
```

- The other files on the Flash – If the first file in the Flash is not the Cisco IOS Software image, but a configuration file or something else, then you need to configure a **boot system** statement in order to boot the specified image. Otherwise, the router will try to boot with the configuration file or the first file in the Flash; this will not work. If there is only one file in the Flash which is the Cisco IOS Software image, then this step is not necessary.

```
2610#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
2610(config)#no boot system
2610(config)#boot system flash c2600-i-mz.121-14.bin
2610(config)#^Z
```

Note: If you type the **reload** command, the router asks you if you want to save the configuration. You should be very cautious here. The reason is that if the router is in boot mode for instance, it is a subset of the full Cisco IOS software which is running and there is no routing functionality. Therefore, all the routing configuration is gone in the running configuration and if you save the configuration at this time, then you erase the good startup-configuration in NVRAM and replace it by the incomplete running-configuration. Save the configuration only if you are sure that you have the full configuration in the output of **show run**. It is *not* necessary to save the configuration to take into account the new configuration register if this one has been changed previously. That is done automatically.

```
2610#reload

System configuration has been modified. Save? [yes/no]: y
Building configuration...
[OK]
Proceed with reload? [confirm]y
```

Verify that the router is running with the proper image. After the reload is complete, the router should be running the desired Cisco IOS Software image. Use the **show version** command to verify.

```
2610#show version
00:22:25: %SYS-5-CONFIG_I: Configured from console by console
Cisco Internetwork Operating System Software
IOS (tm) C2600 Software (C2600-I-M), Version 12.1(14), RELEASE SOFTWARE (fc1)
Copyright (c) 1986-2002 by cisco Systems, Inc.
Compiled Mon 25-Mar-02 20:33 by kellythw
Image text-base: 0x80008088, data-base: 0x80828788

ROM: System Bootstrap, Version 11.3(2)XA4, RELEASE SOFTWARE (fc1)

2610 uptime is 22 minutes
System returned to ROM by reload
System image file is "flash:c2600-i-mz.121-14.bin"
```

Upgrade Procedure for Cisco 3600 Series Routers with PCMCIA Cards

- Establish a console session to the router
- Verify the amount of free space on the Flash memory card (PCMCIA slot)
- Verify that the TFTP server has IP connectivity to the router
- Copy the new image into the Flash memory card through the TFTP server
- Set boot statements to load the new image upon startup
- Reboot the router to load the new image
- Verify the upgrade

Establish a console session to the router

See Establish a console session to the router for more information.

Note: Once connected to the router through the console port, if you get a ">" or "rommon >" prompt, your router is in ROM monitor (ROMmon) mode. If the router is showing the "router (boot)>" prompt, then the router is in boot mode. See booting problems for steps to handle either of these situations.

Verify the amount of free space on the Flash memory card (PCMCIA slot)

At this point, you need to verify that you have enough space in the Flash memory card to copy the new image. If there is not enough memory, you need to delete some files to make enough space. In some situations, if the image is very large, you may need to delete the current image in the Flash memory card.

To determine the amount of free space, and to show files currently located in slot0: or slot1:, issue the **dir{*device:*}** command.

```
3600#dir slot1:
Directory of slot1:/

  1  -rw-     2779832    c3640-i-mz.113-11c.bin
  2  -rw-     3748760    c3640-i-mz.120-22.bin
```

Verify that the name and the file size are correct.

If you find that there is not enough space, you can delete the file. The **delete{*device:*}[*filename*]** command deletes the file.

```
3600#delete slot1:
Delete filename []? c3640-i-mz.113-11c.bin
Delete slot1:c3640-i-mz.113-11c.bin? [confirm]y
```

Note: Do not reload or powercycle the router if there is not a valid image in the Flash; this causes the router to boot into rommon or bootmode.

Verify that the TFTP server has IP connectivity to the router

The TFTP server must have a network connection to the router and must be able to ping the IP address of the router targeted for a TFTP software upgrade. To achieve this, the router interface and the TFTP server must have:

23.886
A

- an IP address in the same range, or
- a default gateway configured

To verify this, check the IP address of the TFTP server.

See Determining IP Addresses for more details.

Copy the new image into the Flash memory card through the TFTP server

Now that you have IP connectivity and can ping between the computer acting as a TFTP server and the router, you can copy the image into the right slot.

Note: Before copying, make sure you have started the TFTP server software on your PC and that you have the filename mentioned in the TFTP server root directory. We recommend that you keep a backup of the router/access server configuration before upgrading. The upgrade itself does not affect the configuration (which is stored in nonvolatile RAM –NVRAM). However, this may happen if the right steps are not followed properly.

For RCP applications, substitute RCP for every occurrence of TFTP. For example, use the **copy rcp {*device:*}** command instead of the **copy tftp {*device:*}** command.

If necessary, you can copy an image from one device to another.

```
3600#copy tftp: slot1:
Address or name of remote host []? 171.68.173.10
Source filename []? c3640-i-mz.122-7b.bin
Destination filename [c3640-i-mz.122-7b.bin]?
Accessing tftp://171.68.173.10/c3640-i-mz.122-7b.bin...
Erase slot1: before copying? [confirm]n
!--- Here you are specifying "n"


!--- because there is enough memory available.

Loading c3640-i-mz.122-7b.bin from 171.68.173.10 (via Ethernet1/0):
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!
[OK - 5996844/11993088 bytes]

Verifying checksum...  OK (0x13F0)
5996844 bytes copied in 67.708 secs (89505 bytes/sec)
3600#
```

Use the **dir slot1:** command to check whether the image has been copied to slot1. Below, you can see that the new image **c3640–i–mz.122–7b.bin** has been copied on the PCMCIA slot1:

```
3600#dir slot1:
Directory of slot1:/

  2  -rw-     3748760    c3640-i-mz.120-22.bin
```

```
3   -rw-     5996844     c3640-i-mz.122-7b.bin
```

Set boot statements to load the new image upon startup

After copying the image through TFTP, you may need to tell the router which image to load upon boot up.

Checking Current Boot Statements

At this point, the new image is now in the slot1. You need to set the router to boot the new image. By default, the router boots the first available image (the default is enabled when there are no boot statements in the configuration).

```
3600#show running-config
Building configuration...

Current configuration:
!
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname 3600
!
boot system flash slot1:c3640-i-mz.120-22.bin
!
ip subnet-zero
!
```

The commands appear at the begginning of the configuration. In our example above, it shows the router has a **boot system** command configured as **boot system flash slot1:c3640–i–mz.120–22.bin**.

If you have **boot system** command entries in your configuration, you need to remove them from the configuration. For more information on removing boot entries, refer to the next section.

Removing Previous Boot Statements

To remove the commands, enter into configuration terminal mode. From the configuration mode, you can negate any command by typing "no" in front of each boot statement. The following example illustrates the removal of an existing boot statement.

```
3600#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
3600(config)#no boot system flash slot1:c3640-i-mz.120-22.bin
3600(config)#^Z
3600#
```

The statement "**no boot system flash slot1:c3640–i–mz.120–22.bin**" is removed from the configuration. Verify that the command has been removed by issuing the **show running–config** command.

Setting New Boot Statements

Now set the router to boot the new image. Issue the following command to set the boot system parameter:

```
boot system flash slot#:{imagename} (imagename = name of the new Cisco IOS software image)

3600#configure terminal
```

```
Enter configuration commands, one per line.  End with CNTL/Z.
3600(config)#boot system flash slot1:c3640-i-mz.122-7b.bin
3600(config)#^Z
3600#write memory
3d01h: %SYS-5-CONFIG_I: Configured from console by vty0
Building configuration...
3600#
```

Be sure to verify that you are using **config–register 0x2102** by issuing the **show version** command. If it is set up differently, you can change it by issuing the following command in configuration mode:

```
3600#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
3600(config)#config-register 0x2102
3600(config)#^Z
```

After changing the config–register, the change takes place at the next reload.

Reboot the router to load the new image

For the router to run the new Cisco IOS software image, you need to reload the router. Make sure you have saved the configuration by issuing the **copy running–config starting–config** or **write memory** commands.

```
3600#write memory
3d01h: %SYS-5-CONFIG_I: Configured from console by vty0 (127.0.0.11)
Building configuration...
3600#reload
```

Verify the upgrade

After the router comes up, make sure you are currently running the new version of code, by issuing the **show version** command.

```
3640#show version
Cisco Internetwork Operating System Software
IOS (tm) 3600 Software (C3640-I-M), Version 12.2(7b), RELEASE SOFTWARE (fc1)
Copyright (c) 1986-2002 by cisco Systems, Inc.
Compiled Mon 04-Mar-02 20:23 by pwade
Image text-base: 0x600089A8, data-base: 0x60A6A000

ROM: System Bootstrap, Version 11.1(19)AA, EARLY DEPLOYMENT RELEASE SOFTWARE (f)

Router uptime is 2 minutes
System returned to ROM by reload
System image file is "slot1:c3640-i-mz.122-7b.bin"

cisco 3640 (R4700) processor (revision 0x00) with 59392K/6144K bytes of memory.

Processor board ID 10524422
R4700 CPU at 100Mhz, Implementation 33, Rev 1.0
Bridging software.
X.25 software, Version 3.0.0.
4 Ethernet/IEEE 802.3 interface(s)
DRAM configuration is 64 bits wide with parity disabled.
125K bytes of non-volatile configuration memory.
4096K bytes of processor board System flash (Read/Write)
20480K bytes of processor board PCMCIA Slot0 flash (Read/Write)
20480K bytes of processor board PCMCIA Slot1 flash (Read/Write)

Configuration register is 0x2102
```

Verify that the version 12.2(7b) is correct and that the configuration register is set to 0x2102.

Related Information

- **How to Choose a Cisco IOS Software Release**
- **The ABCs of Cisco IOS Software**
- **Cisco IOS Software Roadmap**
- **PCMCIA Flash Compatibility Matrix and Filesystem Information**
- **Field Notice: Cisco IOS TFTP Client Cannot Transfer Files Larger than 16MB in Size**
- **Technical Support – Cisco Systems**

redistribute (BGP to ISO IS-IS)

To redistribute routes from a Border Gateway Protocol (BGP) autonomous system into an International Organization for Standardization (ISO) Intermediate System-to-Intermediate System (IS-IS) routing process, use the **redistribute** command in router configuration mode. To remove the **redistribute** command from the configuration file and restore the system to its default condition where the software does not redistribute routes, use the **no** form of this command.

redistribute *protocol as-number* [*route-type*] [**route-map** *map-tag*]

no redistribute *protocol as-number* [*route-type*] [**route-map** *map-tag*]

Syntax Description

protocol	Source protocol from which routes are being redistributed. It must be the **bgp** keyword. The **bgp** keyword is used to redistribute dynamic routes.
as-number	The autonomous system number of the BGP routing process.
route-type	(Optional) The type of route to be redistributed. It can be one of the following keywords: **clns** or **ip**. The default is **ip.** The **clns** keyword is used to redistribute BGP routes with network service access point (NSAP) addresses into IS-IS. The **ip** keyword is used to redistribute BGP routes with IP addresses into IS-IS.
route-map *map-tag*	(Optional) Identifier of a configured route map. The route map should be examined to filter the importation of routes from this source routing protocol to IS-IS. If not specified, all routes are redistributed. If the keyword is specified, but no route map tags are listed, no routes will be imported.

Defaults

Route redistribution is disabled.

protocol: No source protocol is defined.
route-type: **ip**
route-map *map-tag*: If the **route-map** argument is not entered, all routes are redistributed; if no *map-tag* value is entered, no routes are imported.

Command Modes

Router configuration

Command History

Release	Modification
12.2(8)T	The **clns** keyword was added.

Usage Guidelines

The **clns** keyword must be specified to redistribute NSAP prefix routes from BGP into an ISO IS-IS routing process. This version of the **redistribute** command is used only under router configuration mode for IS-IS processes.

Examples

The following example configures NSAP prefix routes from BGP autonomous system 64500 to be redistributed into the IS-IS routing process called osi-proc-17:

```
router isis osi-proc-17
 redistribute bgp 64500 clns
```

Related Commands

Command	Description
network (BGP and multiprotocol BGP)	Specifies the list of networks for the BGP routing process.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another.
show route-map	Displays all route maps configured or only the one specified.

redistribute (IP)

To redistribute routes from one routing domain into another routing domain, use the **redistribute** command in router configuration mode. To disable redistribution, use the **no** form of this command.

redistribute *protocol* [*process-id*] {**level-1** | **level-1-2** | **level-2**} [*as-number*] [**metric** *metric-value*] [**metric-type** *type-value*] [**match** {**internal** | **external 1** | **external 2**}] [**tag** *tag-value*] [**route-map** *map-tag*] [**subnets**]

no redistribute *protocol* [*process-id*] {**level-1** | **level-1-2** | **level-2**} [*as-number*] [**metric** *metric-value*] [**metric-type** *type-value*] [**match** {**internal** | **external 1** | **external 2**}] [**tag** *tag-value*] [**route-map** *map-tag*] [**subnets**]

Syntax Description

protocol	Source protocol from which routes are being redistributed. It can be one of the following keywords: **bgp**, **connected**, **egp**, **igrp**, **isis**, **mobile**, **ospf**, **static [ip]**, or **rip**. The **static [ip]** keyword is used to redistribute IP static routes. The optional **ip** keyword is used when redistributing into the Intermediate System-to-Intermediate System (IS-IS) protocol. The **connected** keyword refers to routes that are established automatically by virtue of having enabled IP on an interface. For routing protocols such as Open Shortest Path First (OSPF) and IS-IS, these routes will be redistributed as external to the autonomous system.
process-id	(Optional) For the **bgp**, **egp**, or **igrp** keyword, this is an autonomous system number, which is a 16-bit decimal number. For the **isis** keyword, this is an optional *tag* value that defines a meaningful name for a routing process. You can specify only one IS-IS process per router. Creating a name for a routing process means that you use names when configuring routing. For the **ospf** keyword, this is an appropriate OSPF process ID from which routes are to be redistributed. This identifies the routing process. This value takes the form of a nonzero decimal number. For the **rip** keyword, no *process-id* value is needed.
level-1	Specifies that for IS-IS Level 1 routes are redistributed into other IP routing protocols independently.
level-1-2	Specifies that for IS-IS both Level 1 and Level 2 routes are redistributed into other IP routing protocols.
level-2	Specifies that for IS-IS Level 2 routes are redistributed into other IP routing protocols independently.
as-number	(Optional) Autonomous system number for the redistributed route.
metric *metric-value*	(Optional) When redistributing from one OSPF process to another OSPF process on the same router, the metric will be carried through from one process to the other if no metric value is specified. When redistributing other processes to an OSPF process, the default metric is 20 when no metric value is specified.

metric-type *type-value*	(Optional) For OSPF, the external link type associated with the default route advertised into the OSPF routing domain. It can be one of two values: • **1**—Type 1 external route • **2**—Type 2 external route If a **metric-type** is not specified, the Cisco IOS software adopts a Type 2 external route. For IS-IS, it can be one of two values: • **internal**—IS-IS metric that is < 63. • **external**—IS-IS metric that is > 64 < 128. The default is **internal**.
match {internal | external 1 | external 2}	(Optional) For the criteria by which OSPF routes are redistributed into other routing domains. It can be one of the following: • **internal**—Routes that are internal to a specific autonomous system. • **external 1**—Routes that are external to the autonomous system, but are imported into OSPF as Type 1 external route. • **external 2**—Routes that are external to the autonomous system, but are imported into OSPF as Type 2 external route.
tag *tag-value*	(Optional) 32-bit decimal value attached to each external route. This is not used by OSPF itself. It may be used to communicate information between Autonomous System Boundary Routers (ASBRs). If none is specified, then the remote autonomous system number is used for routes from Border Gateway Protocol (BGP) and Exterior Gateway Protocol (EGP); for other protocols, zero (0) is used.
route-map	(Optional) Route map that should be interrogated to filter the importation of routes from this source routing protocol to the current routing protocol. If not specified, all routes are redistributed. If this keyword is specified, but no route map tags are listed, no routes will be imported.
map-tag	(Optional) Identifier of a configured route map.
subnets	(Optional) For redistributing routes into OSPF, the scope of redistribution for the specified protocol.

Defaults

Route redistribution is disabled.

protocol: No source protocol is defined.

process-id: No process ID is defined.

metric *metric-value*: 0

metric-type *type-value*: Type 2 external route

match internal | external: Internal, external 1, external 2

external: Internal

tag *tag-value*: If no value is specified, the remote autonomous system number is used for routes from BGP and EGP; for other protocols, the default is 0.

route-map *map-tag*: If the **route-map** keyword is not entered, all routes are redistributed; if no *map-tag* value is entered, no routes are imported.

subnets: No subnets are defined.

Command Modes

Router configuration

Address family configuration

Command History

Release	Modification
10.0	This command was introduced.
12.0(5)T	Address family configuration mode was added.
12.0(22)S	Address family support under EIGRP was added in Cisco IOS Release 12.0(22)S.
12.2(15)T	Address family support under EIGRP was added in Cisco IOS Release 12.2(15)T.

Usage Guidelines

Changing or disabling any keyword will not affect the state of other keywords.

A router receiving a link-state protocol with an internal metric will consider the cost of the route from itself to the redistributing router plus the advertised cost to reach the destination. An external metric only considers the advertised metric to reach the destination.

Routes learned from IP routing protocols can be redistributed at Level 1 into an attached area or at Level 2. The **level-1-2** keyword allows both Level 1 and Level 2 routes in a single command.

Redistributed routing information must be filtered by the **distribute-list out** router configuration command. This guideline ensures that only those routes intended by the administrator are passed along to the receiving routing protocol.

Whenever you use the **redistribute** or the **default-information** router configuration commands to redistribute routes into an OSPF routing domain, the router automatically becomes an ASBR. However, an ASBR does not, by default, generate a *default route* into the OSPF routing domain.

When routes are redistributed between OSPF processes, no OSPF metrics are preserved.

When routes are redistributed into OSPF and no metric is specified in the **metric** keyword, OSPF uses the default metric 20 for routes from all protocols except BGP, which gets a metric of 1. Furthermore, when the router redistributes from one OSPF process to another OSPF process on the same router, and if no default metric is specified, the metrics in one process are carried to the redistributing process.

When routes are redistributed into OSPF, only routes that are not subnetted are redistributed if the **subnets** keyword is not specified.

Routes configured with the **connected** keyword affected by this **redistribute** command are the routes not specified by the **network** router configuration command.

You cannot use the **default-metric** command to affect the metric used to advertise **connected** routes.

Note The **metric** value specified in the **redistribute** command supersedes the **metric** value specified using the **default-metric** command.

Default redistribution of IGPs or EGP into BGP is not allowed unless the **default-information originate** router configuration command is specified.

Examples

The following example causes OSPF routes to be redistributed into a BGP domain:

```
router bgp 109
 redistribute ospf
```

The following example causes Interior Gateway Routing Protocol (IGRP) routes to be redistributed into an OSPF domain:

```
router ospf 110
 redistribute igrp
```

The following example causes the specified IGRP process routes to be redistributed into an OSPF domain. The IGRP-derived metric will be remapped to 100 and RIP routes to 200.

```
router ospf 109
 redistribute igrp 108 metric 100 subnets
 redistribute rip metric 200 subnets
```

The following example configures BGP routes to be redistributed into IS-IS. The link-state cost is specified as 5, and the metric type will be set to external, indicating that it has lower priority than internal metrics.

```
router isis
 redistribute bgp 120 metric 5 metric-type external
```

In the following example, network 172.16.0.0 will appear as an external link-state advertisement (LSA) in OSPF 1 with a cost of 100 (the cost is preserved):

```
interface ethernet 0
 ip address 172.16.0.1 255.0.0.0
 ip ospf cost 100
interface ethernet 1
 ip address 10.0.0.1 255.0.0.0
!
router ospf 1
 network 10.0.0.0 0.255.255.255 area 0
 redistribute ospf 2 subnet
router ospf 2
 network 172.16.0.0 0.255.255.255 area 0
```

Related Commands

Command	Description
address-family ipv4 (BGP)	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard IPv4 address prefixes.
address-family vpnv4	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard VPNv4 address prefixes.

Command	Description
default-information originate (BGP)	Allows the redistribution of network 0.0.0.0 into BGP.
default-information originate (IS-IS)	Generates a default route into an IS-IS routing domain.
default-information originate (OSPF)	Generates a default route into an OSPF routing domain.
distribute-list out (IP)	Suppresses networks from being advertised in updates.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.
show route-map	Displays all route maps configured or only the one specified.

redistribute (ISO ISIS to BGP)

To redistribute routes from an International Organization for Standardization (ISO) Intermediate System-to-Intermediate System (IS-IS) routing process into a Border Gateway Protocol (BGP) autonomous system, use the **redistribute** command in router configuration mode. To remove the **redistribute** command from the configuration file and restore the system to its default condition where the software does not redistribute routes, use the **no** form of this command.

redistribute *protocol* [*process-id*] [*route-type*] [**route-map** *map-tag*]

no redistribute *protocol* [*process-id*] [*route-type*] [**route-map** *map-tag*]

Syntax Description

protocol	Source protocol from which routes are being redistributed. It can be one of the following keywords: **isis** or **static**. The **isis** keyword is used to redistribute dynamic routes. The **static** keyword is used to redistribute static routes.
process-id	(Optional) When IS-IS is used as a source protocol, this argument defines a meaningful name for a routing process. The *process-id* argument identifies from which IS-IS routing process routes will be redistributed. Routes can be redistributed only from IS-IS routing processes that involve Level 2 routes, including IS-IS Level 1-2 and Level 2 routing processes. The *process-id* argument is not used when the protocol keyword is **static**.
route-type	(Optional) The type of route to be redistributed. It can be one of the following keywords: **clns** or **ip**. The default is **ip**. The **clns** keyword is used to redistribute Connectionless Network Service (CLNS) routes with network service access point (NSAP) addresses into BGP. The **ip** keyword is used to redistribute IS-IS routes with IP addresses into BGP.
route-map *map-tag*	(Optional) Identifier of a configured route map. The route map should be examined to filter the importation of routes from this source routing protocol to BGP. If no route map is specified, all routes are redistributed. If the keyword is specified, but no route map tags are listed, no routes will be imported.

Defaults

Route redistribution is disabled.

protocol: No source protocol is defined.
route-type: **ip**
route-map *map-tag*: If the **route-map** argument is not entered, all routes are redistributed; if no *map-tag* value is entered, no routes are imported.

Command Modes

Router configuration

Command History

Release	Modification
12.2(8)T	The **clns** keyword was added.

Usage Guidelines

The **clns** keyword must be specified to redistribute NSAP prefix routes from an ISO IS-IS routing process into BGP. This version of the **redistribute** command is used only under router configuration mode for BGP processes.

Examples

The following example configures CLNS NSAP routes from the IS-IS routing process called osi-proc-6 to be redistributed into BGP:

```
router bgp 64352
 redistribute isis osi-proc-6 clns
```

Related Commands

Command	Description
network (BGP and multiprotocol BGP)	Specifies the list of networks for the BGP routing process.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another.
show route-map	Displays all route maps configured or only the one specified.

redistribute dvmrp

To configure redistribution of Distance Vector Multicast Routing Protocol (DVMRP) routes into multiprotocol BGP, use the **redistribute dvmrp** command in address family or router configuration mode. To stop such redistribution, use the **no** form of this command.

redistribute dvmrp [**route-map** *map-name*]

no redistribute dvmrp [**route-map** *map-name*]

Syntax Description

route-map *map-name*	(Optional) Name of the route map that contains various BGP attribute settings.

Defaults

DVMRP routes are not redistributed into multiprotocol BGP.

Command Modes

Address family configuration

Router configuration

Command History

Release	Modification
11.1(20)CC	This command was introduced.
12.0(7)T	Address family configuration mode was added.

Usage Guidelines

Use this command if you have a subset of DVMRP routes in an autonomous system that you want to take the multiprotocol BGP path. Define a route map to further specify which DVMRP routes get redistributed.

Examples

The following router configuration mode example redistributes DVMRP routes to BGP peers that match access list 1:

```
router bgp 109
 redistribute dvmrp route-map dvmrp-into-mbgp
route-map dvmrp-into-mbgp
 match ip address 1
```

The following address family configuration mode example redistributes DVMRP routes to multiprotocol BGP peers that match access list 1:

```
router bgp 109
address-family ipv4 multicast
 redistribute dvmrp route-map dvmrp-into-mbgp

route-map dvmrp-into-mbgp
 match ip address 1
```

Configuring BGP

This chapter describes how to configure Border Gateway Protocol (BGP). For a complete description of the BGP commands in this chapter, refer to the "BGP Commands" chapter of the *Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols*. To locate documentation of other commands that appear in this chapter, use the command reference master index, or search online. For multiprotocol BGP configuration information and examples, refer to the "Configuring Multiprotocol BGP Extensions for IP Multicast" chapter of the *Cisco IOS IP Configuration Guide*. For multiprotocol BGP command descriptions, refer to the "Multiprotocol BGP Extensions for IP Multicast Commands" chapter of the *Cisco IOS IP Command Reference*.

BGP, as defined in RFCs 1163 and 1267, is an Exterior Gateway Protocol (EGP). It allows you to set up an interdomain routing system that automatically guarantees the loop-free exchange of routing information between autonomous systems.

For protocol-independent features, see the chapter "Configuring IP Routing Protocol-Independent Features" in this book.

To identify the hardware platform or software image information associated with a feature, use the Feature Navigator on Cisco.com to search for information about the feature or refer to the software release notes for a specific release. For more information, see the "Identifying Supported Platforms" section in the "Using Cisco IOS Software" chapter in this book.

The Cisco BGP Implementation

In BGP, each route consists of a network number, a list of autonomous systems that information has passed through (called the *autonomous system path*), and a list of other *path attributes*. We support BGP Versions 2, 3, and 4, as defined in RFCs 1163, 1267, and 1771, respectively.

The primary function of a BGP system is to exchange network reachability information with other BGP systems, including information about the list of autonomous system paths. This information can be used to construct a graph of autonomous system connectivity from which routing loops can be pruned and with which autonomous system-level policy decisions can be enforced.

You can configure the value for the Multi Exit Discriminator (MED) metric attribute using route maps. (The name of this metric for BGP Versions 2 and 3 is INTER_AS_METRIC.) When an update is sent to an internal BGP (iBGP) peer, the MED is passed along without any change. This action enables all the peers in the same autonomous system to make a consistent path selection.

A next hop router address is used in the NEXT_HOP attribute, regardless of the autonomous system of that router. The Cisco IOS software automatically calculates the value for this attribute.

Transitive, optional path attributes are passed along to other BGP-speaking routers.

BGP Version 4 supports classless interdomain routing (CIDR), which lets you reduce the size of your routing tables by creating aggregate routes, resulting in *supernets*. CIDR eliminates the concept of network classes within BGP and supports the advertising of IP prefixes. CIDR routes can be carried by Open Shortest Path First (OSPF), Enhanced IGRP (EIGRP), and Intermediate System-to-Intermediate System (ISIS)-IP, and Routing Information Protocol (RIP).

See the "BGP Route Map Examples" section at the end of this chapter for examples of how to use route maps to redistribute BGP Version 4 routes.

How BGP Selects Paths

A router running Cisco IOS Release 12.0 or later does not select or use an iBGP route unless both of the following conditions are true:

- The router has a route available to the next hop router:
- The router has received synchronization via an IGP (unless IGP synchronization has been disabled).

BGP bases its decision process on the attribute values. When faced with multiple routes to the same destination, BGP chooses the best route for routing traffic toward the destination. The following process summarizes how BGP chooses the best route.

1. If the next hop is inaccessible, do not consider it.

   This decision is why it is important to have an IGP route to the next hop.
2. If the path is internal, synchronization is enabled, and the route is not in the IGP, do not consider the route.
3. Prefer the path with the largest weight (weight is a Cisco proprietary parameter).
4. If the routes have the same weight, prefer the route with the largest local preference.
5. If the routes have the same local preference, prefer the route that was originated by the local router.

   For example, a route might be originated by the local router using the **network bgp** router configuration command, or through redistribution from an IGP.
6. If the local preference is the same, or if no route was originated by the local router, prefer the route with the shortest autonomous system path.
7. If the autonomous system path length is the same, prefer the route with the lowest origin code (IGP < EGP < INCOMPLETE).
8. If the origin codes are the same, prefer the route with the lowest MED metric attribute.

   This comparison is only made if the neighboring autonomous system is the same for all routes considered, unless the **bgp always-compare-med** router configuration command is enabled.

   Note The most recent Internet Engineering Task Force (IETF) decision regarding BGP MED assigns a value of infinity to the missing MED, making the route lacking the MED variable the least preferred. The default behavior of BGP routers running Cisco IOS software is to treat routes without the MED attribute as having a MED of 0, making the route lacking the MED variable the most preferred. To configure the router to conform to the IETF standard, use the **bgp bestpath med missing-as-worst** router configuration command.
9. Prefer the external BGP (eBGP) path over the iBGP path.

   All confederation paths are considered internal paths.

10. Prefer the route that can be reached through the closest IGP neighbor (the lowest IGP metric).

    The router will prefer the shortest internal path within the autonomous system to reach the destination (the shortest path to the BGP next hop).

11. If the following conditions are all true, insert the route for this path into the IP routing table:
    - Both the best route and this route are external.
    - Both the best route and this route are from the same neighboring autonomous system.
    - The **maximum-paths** router configuration command is enabled.

    Note eBGP load sharing can occur at this point, which means that multiple paths can be installed in the forwarding table.

12. If multipath is not enabled, prefer the route with the lowest IP address value for the BGP router ID.

    The router ID is usually the highest IP address on the router or the loopback (virtual) address, but might be implementation-specific.

BGP Multipath Support

When a BGP speaker learns two identical eBGP paths for a prefix from a neighboring autonomous system, it will choose the path with the lowest route ID as the best path. This best path is installed in the IP routing table. If BGP multipath support is enabled and the eBGP paths are learned from the same neighboring autonomous system, instead of one best path being picked, multiple paths are installed in the IP routing table.

During packet switching, depending on the switching mode, either per-packet or per-destination load balancing is performed among the multiple paths. A maximum of six paths is supported. The **maximum-paths** router configuration command controls the number of paths allowed. By default, BGP will install only one path to the IP routing table.

Basic BGP Configuration Task List

The BGP configuration tasks are divided into basic and advanced tasks, which are described in the following sections. The basic tasks described in the first two sections are required to configure BGP; the basic and advanced tasks in the remaining sections are optional:

- Enabling BGP Routing (Required)
- Configuring BGP Neighbors (Required)
- Managing Routing Policy Changes (Optional)
- Verifying BGP Soft Reset (Optional)
- Configuring BGP Interactions with IGPs (Optional)
- Configuring BGP Weights (Optional)
- Disabling Autonomous System Path Comparison (Optional)
- Configuring BGP Route Filtering by Neighbor (Optional)
- Configuring BGP Filtering Using Prefix Lists (Optional)
- Configuring BGP Path Filtering by Neighbor (Optional)

- Disabling Next Hop Processing on BGP Updates (Optional)
- Configuring the BGP Version (Optional)
- Configuring the MED Metric (Optional)

Advanced BGP Configuration Task List

Advanced, optional BGP configuration tasks are described in the following sections:

- Using Route Maps to Modify Updates (Optional)
- Resetting eBGP Connections Immediately upon Link Failure (Optional)
- Configuring Aggregate Addresses (Optional)
- Disabling Automatic Summarization of Network Numbers (Optional)
- Configuring BGP Community Filtering (Optional)
- Configuring BGP Conditional Advertisement (Optional)
- Configuring a Routing Domain Confederation (Optional)
- Configuring a Route Reflector (Optional)
- Configuring BGP Peer Groups (Optional)
- Disabling a Peer or Peer Group (Optional)
- Indicating Backdoor Routes (Optional)
- Modifying Parameters While Updating the IP Routing Table (Optional)
- Setting Administrative Distance (Optional)
- Adjusting BGP Timers (Optional)
- Changing the Default Local Preference Value (Optional)
- Redistributing Network 0.0.0.0 (Optional)
- Configuring the Router to Consider a Missing MED as Worst Path (Optional)
- Selecting Path Based on MEDs from Other Autonomous Systems (Optional)
- Configuring the Router to Use the MED to Choose a Path from Subautonomous System Paths (Optional)
- Configuring the Router to Use the MED to Choose a Path in a Confederation (Optional)
- Configuring Route Dampening (Optional)

For information on configuring features that apply to multiple IP routing protocols (such as redistributing routing information), see the chapter "Configuring IP Routing Protocol-Independent Features."

Configuring Basic BGP Features

The tasks described in this section are for configuring basic BGP features.

Enabling BGP Routing

To enable BGP routing and establish a BGP routing process, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# router bgp as-number`	Enables a BGP routing process, which places the router in router configuration mode.
Step 2	`Router(config-router)# network network-number [mask network-mask] [route-map route-map-name]`	Flags a network as local to this autonomous system and enters it to the BGP table.

Note For exterior protocols, a reference to an IP network from the **network** router configuration command controls only which networks are advertised. This behavior is in contrast to IGP, such as IGRP, which also use the **network** command to determine where to send updates.

Note The **network** command is used to inject IGP routes into the BGP table. The *network-mask* portion of the command allows supernetting and subnetting. The resources of the router, such as configured NVRAM or RAM, determine the upper limit of the number of **network** commands you can use. Alternatively, you could use the **redistribute** router configuration command to achieve the same result.

Configuring BGP Neighbors

Like other EGPs, BGP must completely understand the relationships it has with its neighbors. Therefore, this task is required.

BGP supports two kinds of neighbors: internal and external. *Internal neighbors* are in the same autonomous system; *external neighbors* are in different autonomous systems. Normally, external neighbors are adjacent to each other and share a subnet, while internal neighbors may be anywhere in the same autonomous system.

To configure BGP neighbors, use the following command in router configuration mode:

Command	Purpose
`Router(config-router)# neighbor {ip-address | peer-group-name} remote-as as-number`	Specifies a BGP neighbor.

See the "BGP Neighbor Configuration Examples" section at the end of this chapter for an example of configuring BGP neighbors.

Managing Routing Policy Changes

Routing policies for a peer include all the configurations such as route-map, distribute-list, prefix-list, and filter-list that may impact inbound or outbound routing table updates. Whenever there is a change in the routing policy, the BGP session must be soft cleared, or soft reset, for the new policy to take effect. Performing inbound reset enables the new inbound policy to take effect. Performing outbound reset causes the new local outbound policy take effect without resetting the BGP session. As a new set of updates is sent during outbound policy reset, a new inbound policy of the neighbor can also take effect.

There are two types of reset, hard reset and soft reset. Table 8 lists their advantages and disadvantages.

Table 8 Advantages and Disadvantages of Hard and Soft Resets

Type of Reset	Advantages	Disadvantages
Hard reset	No memory overhead.	The prefixes in the BGP, IP, and Forwarding Information Base (FIB) tables provided by the neighbor are lost. Not recommended.
Outbound soft reset	No configuration, no storing of routing table updates. The procedure for an outbound reset is described in the section "Configuring BGP Soft Reset Using Stored Routing Policy Information."	Does not reset inbound routing table updates.
Dynamic inbound soft reset	Does not clear the BGP session and cache. Does not require storing of routing table updates, and has no memory overhead.	Both BGP routers must support the route refresh capability (in Cisco IOS Release 12.1 and later releases).
Configured inbound soft reset (uses the **neighbor soft-reconfiguration** router configuration command)	Can be used when both BGP routers do not support the automatic route refresh capability.	Requires preconfiguration. Stores all received (inbound) routing policy updates without modification; is memory-intensive. Recommended only when absolutely necessary, such as when both BGP routers do not support the automatic route refresh capability.

Once you have defined two routers to be BGP neighbors, they will form a BGP connection and exchange routing information. If you subsequently change a BGP filter, weight, distance, version, or timer, or make a similar configuration change, you must reset BGP connections for the configuration change to take effect.

A soft reset updates the routing table for inbound and outbound routing updates. Cisco IOS software Release 12.1 and later releases support soft reset without any prior configuration. This soft reset allows the dynamic exchange of route refresh requests and routing information between BGP routers, and the subsequent re-advertisement of the respective outbound routing table. There are two types of soft reset:

- When soft reset is used to generate inbound updates from a neighbor, it is called dynamic inbound soft reset.
- When soft reset is used to send a new set of updates to a neighbor, it is called outbound soft reset.

To use soft reset without preconfiguration, both BGP peers must support the soft route refresh capability, which is advertised in the OPEN message sent when the peers establish a TCP session. Routers running Cisco IOS software releases prior to Release 12.1 do not support the route refresh capability and must clear the BGP session using the **neighbor soft-reconfiguration** router configuration command, described in "Configuring BGP Soft Reset Using Stored Routing Policy Information." Clearing the BGP session in this way will have a negative impact upon network operations and should only be used as a last resort.

Resetting a Router Using BGP Dynamic Inbound Soft Reset

If both the local BGP router and the neighbor router support the route refresh capability, you can perform a dynamic soft inbound reset. This type of reset has the following advantages over a soft inbound reset using stored routing update information:

- Does not require preconfiguration
- Does not require additional memory for storing routing update information

To determine whether a router supports the route refresh capability, use the **show ip bgp neighbors** command in EXEC mode:

Command	Purpose
`Router# show ip bgp neighbors ip-address`	Displays whether a neighbor supports the route refresh capability. If the specified router supports the route refresh capability, the following message is displayed: Received route refresh capability from peer.

If all the BGP routers support the route refresh capability, you can use the dynamic soft reset method for resetting the inbound routing table. To perform a dynamic soft reset of the inbound routing table, use the following command in EXEC mode:

Command	Purpose
`Router# clear ip bgp {* | neighbor-address | peer-group-name} soft in`	Performs a dynamic soft reset on the connection specified in the command. The *neighbor-address* argument specifies the connection to be reset. Use the * keyword to specify that all connections be reset.

See the "BGP Soft Reset Examples" section at the end of this chapter for examples of both types of BGP soft resets.

Resetting a Router Using BGP Outbound Soft Reset

Outbound soft resets do not require any preconfiguration. Using the **soft** keyword specifies that a soft reset be performed. To perform an outbound soft reset, use the following command in EXEC mode:

Command	Purpose
`Router# clear ip bgp {* | neighbor-address | peer-group-name} soft out`	Performs a soft reset on the connection specified in the command. The *neighbor-address* argument specifies the connection to be reset. Use the * keyword to specify that all connections be reset.

Configuring BGP Soft Reset Using Stored Routing Policy Information

If all of the BGP routers in the connection do not support the route refresh capability, use the soft reset method that generates a new set of inbound routing table updates from information previously stored. To initiate storage of inbound routing table updates, you must first preconfigure the router using the **neighbor soft-reconfiguration** router configuration command. The **clear ip bgp EXEC** command initiates the soft reset, which generates a new set of inbound routing table updates using the stored information.

Remember that the memory requirements for storing the inbound update information can become quite large.To configure BGP soft reset using stored routing policy information, use the following commands beginning in router configuration mode:

	Command	Purpose
Step 1	`Router(config-router)# neighbor {ip-address | peer-group-name} soft-reconfiguration inbound`	Resets the BGP session and initiates storage of inbound routing table updates from the specified neighbor or peer group. From that point forward, a copy of the BGP routing table for the specified neighbor or peer group is maintained on the router. The Cisco implementation of BGP supports BGP Versions 2, 3, and 4. If the neighbor does not accept default Version 4, dynamic version negotiation is implemented to negotiate down to Version 2. If you specify a BGP peer group by using the *peer-group-name* argument, all members of the peer group will inherit the characteristic configured with this command.
Step 2	`Router# clear ip bgp {* | neighbor-address | peer-group-name} soft in`	Performs a soft reset on the connection specified in the command, using the stored routing table information for that connection.

See the "BGP Path Filtering by Neighbor Examples" section at the end of this chapter for an example of BGP path filtering by neighbor.

Verifying BGP Soft Reset

To verify whether a soft reset is successful and check information about the routing table and about BGP neighbors, perform the following steps:

Step 1 Enter the **show ip bgp** EXEC command to display entries in the BGP routing table. The following output shows that the peer supports the route refresh capability:

```
Router# show ip bgp

BGP table version is 5, local router ID is 10.0.33.34
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 1.0.0.0          0.0.0.0                  0         32768 ?
*  2.0.0.0          10.0.33.35              10             0 35 ?
*>                  0.0.0.0                  0         32768 ?
*  10.0.0.0         10.0.33.35              10             0 35 ?
*>                  0.0.0.0                  0         32768 ?
*> 192.168.0.0/16   10.0.33.35              10             0 35 ?
```

Step 2 Enter the **show ip bgp neighbors** EXEC command to display information about the BGP and TCP connections to neighbors:

```
Router# show ip bgp neighbors 171.69.232.178

BGP neighbor is 172.16.232.178,  remote AS 35, external link
  BGP version 4, remote router ID 192.168.3.3
  BGP state = Established, up for 1w1d
  Last read 00:00:53, hold time is 180, keepalive interval is 60 seconds
  Neighbor capabilities:
    Route refresh: advertised and received
    Address family IPv4 Unicast: advertised and received
    Address family IPv4 Multicast: advertised and received
  Received 12519 messages, 0 notifications, 0 in queue
  Sent 12523 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 30 seconds

 For address family: IPv4 Unicast
  BGP table version 5, neighbor version 5
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor
  Inbound path policy configured
  Outbound path policy configured
  Route map for incoming advertisements is uni-in
  Route map for outgoing advertisements is uni-out
  3 accepted prefixes consume 108 bytes
  Prefix advertised 6, suppressed 0, withdrawn 0

 For address family: IPv4 Multicast
  BGP table version 5, neighbor version 5
  Index 1, Offset 0, Mask 0x2
  Inbound path policy configured
  Outbound path policy configured
  Route map for incoming advertisements is mul-in
  Route map for outgoing advertisements is mul-out
  3 accepted prefixes consume 108 bytes
  Prefix advertised 6, suppressed 0, withdrawn 0

  Connections established 2; dropped 1
  Last reset 1w1d, due to Peer closed the session
```

```
Connection state is ESTAB, I/O status: 1, unread input bytes: 0
Local host: 172.16.232.178, Local port: 179
Foreign host: 172.16.232.179, Foreign port: 11002

Enqueued packets for retransmit: 0, input: 0  mis-ordered: 0 (0 bytes)

Event Timers (current time is 0x2CF49CF8):
Timer          Starts    Wakeups            Next
Retrans         12518          0             0x0
TimeWait            0          0             0x0
AckHold         12514      12281             0x0
SendWnd             0          0             0x0
KeepAlive           0          0             0x0
GiveUp              0          0             0x0
PmtuAger            0          0             0x0
DeadWait            0          0             0x0

iss:  273358651  snduna:  273596614  sndnxt:  273596614     sndwnd:  15434
irs:  190480283  rcvnxt:  190718186  rcvwnd:      15491  delrcvwnd:    893

SRTT: 300 ms, RTTO: 607 ms, RTV: 3 ms, KRTT: 0 ms
minRTT: 0 ms, maxRTT: 300 ms, ACK hold: 200 ms
Flags: passive open, nagle, gen tcbs

Datagrams (max data segment is 1460 bytes):
Rcvd: 24889 (out of order: 0), with data: 12515, total data bytes: 237921
Sent: 24963 (retransmit: 0), with data: 12518, total data bytes: 237981
```

Configuring BGP Interactions with IGPs

If your autonomous system will be passing traffic through it from another autonomous system to a third autonomous system, make sure that your autonomous system is consistent about the routes that it advertises. For example, if your BGP were to advertise a route before all routers in your network had learned about the route through your IGP, your autonomous system could receive traffic that some routers cannot yet route. To prevent this condition from occurring, BGP must wait until the IGP has propagated routing information across your autonomous system, thus causing BGP to be synchronized with the IGP. Synchronization is enabled by default.

In some cases, you need not synchronize. If you will not be passing traffic from a different autonomous system through your autonomous system, or if all routers in your autonomous system will be running BGP, you can disable synchronization. Disabling this feature can allow you to carry fewer routes in your IGP and allow BGP to converge more quickly. To disable synchronization, use the following command in router configuration mode:

Command	Purpose
`Router(config-router)# no synchronization`	Disables synchronization between BGP and an IGP.

See the "BGP Path Filtering by Neighbor Examples" section at the end of this chapter for an example of BGP synchronization.

In general, you will not want to redistribute most BGP routes into your IGP. A common design is to redistribute one or two routes and to make them exterior routes in IGRP, or have your BGP speaker generate a default route for your autonomous system. When redistributing from BGP into IGP, only the routes learned using eBGP get redistributed.

In most circumstances, you also will not want to redistribute your IGP into BGP. List the networks in your autonomous system with **network** router configuration commands and your networks will be advertised. Networks that are listed this way are referred to as *local networks* and have a BGP origin attribute of "IGP." They must appear in the main IP routing table and can have any source; for example, they can be directly connected or learned via an IGP. The BGP routing process periodically scans the main IP routing table to detect the presence or absence of local networks, updating the BGP routing table as appropriate.

If you do perform redistribution into BGP, you must be very careful about the routes that can be in your IGP, especially if the routes were redistributed from BGP into the IGP elsewhere. Redistributing routes from BGP into the IGP elsewhere creates a situation where BGP is potentially injecting information into the IGP and then sending such information back into BGP, and vice versa. Incorrectly redistributing routes into BGP can result in the loss of critical information, such as the autonomous system path, that is required for BGP to function properly.

Networks that are redistributed into BGP from the EGP protocol will be given the BGP origin attribute "EGP." Other networks that are redistributed into BGP will have the BGP origin attribute of "incomplete." The origin attribute in the Cisco implementation is only used in the path selection process.

Configuring BGP Weights

A weight is a number that you can assign to a path so that you can control the path selection process. The administrative weight is local to the router. A weight can be a number from 0 to 65535. Any path that a Cisco router originates will have a default weight of 32768; other paths have weight 0. If you have particular neighbors that you want to prefer for most of your traffic, you can assign a higher weight to all routes learned from that neighbor.

Weights can be assigned based on autonomous system path access lists. A given weight becomes the weight of the route if the autonomous system path is accepted by the access list. Any number of weight filters are allowed. Weights can only be assigned via route maps.

Disabling Autonomous System Path Comparison

RFC 1771, the IETF document defining BGP, does not include autonomous system path as part of the "tie-breaker" decision algorithm. By default, Cisco IOS software considers the autonomous system path as a part of the decision algorithm. This enhancement makes it possible to modify the decision algorithm, bringing the behavior of the router in selecting a path more in line with the IETF specification.

To prevent the router from considering the autonomous system path length when selecting a route, use the following command in router configuration mode:

Command	Purpose
`Router(config-router)# bgp bestpath as-path ignore`	Configures the router to ignore autonomous system path length in selecting a route.

Configuring BGP Route Filtering by Neighbor

You can filter BGP advertisements in two ways:

- Use autonomous system path filters, as with the **ip as-path access-list** global configuration command and the **neighbor filter-list** router configuration command
- Use access or prefix lists, as with the **neighbor distribute-list** router configuration command.

Filtering using prefix lists is described in the "Configuring BGP Filtering Using Prefix Lists" section.

If you want to restrict the routing information that the Cisco IOS software learns or advertises, you can filter BGP routing updates to and from particular neighbors. You can either define an access list or a prefix list and apply it to the updates.

Note Distribute-list filters are applied to network numbers and not autonomous system paths.

To filter BGP routing updates, use the following command in router configuration mode:

Command	Purpose
`Router(config-router)# neighbor {ip-address | peer-group-name} distribute-list {access-list-number | access-list-name} {in | out}`	Filters BGP routing updates to and from neighbors as specified in an access list. **Note** The **neighbor prefix-list** router configuration command can be used as an alternative to the **neighbor distribute-list** router configuration command, but you cannot use both commands to configure the same BGP peer in any specific direction. These two commands are mutually exclusive, and only one command (**neighbor prefix-list** or **neighbor distribute-list**) an be applied for each inbound or outbound direction.

Note Although the **neighbor prefix-list** router configuration command can be used as an alternative to the **neighbor distribute-list** command, do not use attempt to apply both the **neighbor prefix-list** and **neighbor distribute-list** command filtering to the same neighbor in any given direction. These two commands are mutually exclusive, and only one command (**neighbor prefix-list** or **neighbor distribute-list**) can be applied for each inbound or outbound direction.

Configuring BGP Filtering Using Prefix Lists

Prefix lists can be used as an alternative to access lists in many BGP route filtering commands. The section "How the System Filters Traffic by Prefix List" describes the way prefix list filtering works. The advantages of using prefix lists are as follows:

- Significant performance improvement in loading and route lookup of large lists.
- Support for incremental updates. Filtering using extended access lists does not support incremental updates.

- More user-friendly command-line interface (CLI). The command-line interface for using access lists to filter BGP updates is difficult to understand and use because it uses the packet filtering format.
- Greater flexibility

Before using a prefix list in a command, you must set up a prefix list, and you may want to assign sequence numbers to the entries in the prefix list.

How the System Filters Traffic by Prefix List

Filtering by prefix list involves matching the prefixes of routes with those listed in the prefix list. When there is a match, the route is used. More specifically, whether a prefix is permitted or denied is based upon the following rules:

- An empty prefix list permits all prefixes.
- An implicit deny is assumed if a given prefix does not match any entries of a prefix list.
- When multiple entries of a prefix list match a given prefix, the longest, most specific match is chosen.

  The router begins the search at the top of the prefix list, with the sequence number 1. Once a match or deny occurs, the router need not go through the rest of the prefix list. For efficiency, you may want to put the most common matches or denies near the top of the list, using the **seq** argument in the **ip prefix-list** global configuration command. The **show** commands always include the sequence numbers in their output.

Sequence numbers are generated automatically unless you disable this automatic generation. If you disable the automatic generation of sequence numbers, you must specify the sequence number for each entry using the *sequence-value* argument of the **ip prefix-list** global configuration command.

Regardless of whether the default sequence numbers are used in configuring a prefix list, a sequence number need not be specified when removing a configuration entry.

show commands include the sequence numbers in their output.

Creating a Prefix List

To create a prefix list, use the following command in router configuration mode:

Command	Purpose
`Router(config-router)# ip prefix-list list-name [seq sequence-value] {deny | permit network/length} [ge ge-value] [le le-value]`	Creates a prefix list with the name specified for the *list-name* argument.

Note To create a prefix list you must enter at least one **permit** or **deny** clause.

To remove a prefix list and all of its entries, use the following command in router configuration mode:

Command	Purpose
`Router(config-router)# no ip prefix-list list-name [seq sequence-value] {deny | permit network/length} [ge ge-value] [le le-value]`	Removes a prefix list with the name specified for *list-name*.

Configuring a Prefix List Entry

You can add entries to a prefix list individually. To configure an entry in a prefix list, use the following command in router configuration mode:

Command	Purpose
`Router(config-router)# ip prefix-list` *list-name* `[seq` *sequence-value*`] {deny | permit` *network/length*`} [ge` *ge-value*`] [le` *le-value*`]`	Creates an entry in a prefix list and assigns a sequence number to the entry.

The optional **ge** and **le** keywords can be used to specify the range of the prefix length to be matched for prefixes that are more specific than the *network/length* argument. An exact match is assumed when neither **ge** nor **le** is specified. The range is assumed to be from *ge-value* to 32 if only the **ge** attribute is specified, and from **len** to *le-value* if only the **le** attribute is specified.

A specified *ge-value* or *le-value* must satisfy the following condition:

```
len < ge-value <= le-value <= 32
```

For example, to deny all prefixes matching /24 in 128.0.0.0/8, use the following command:

```
ip prefix-list abc deny  128.0.0.0/8 ge 24 le 24
```

Note You can specify sequence values for prefix list entries in any increments you want (the automatically generated numbers are incremented in units of 5). If you specify the sequence values in increments of 1, you cannot insert additional entries into the prefix list. If you choose very large increments, you could run out of sequence values.

Configuring How Sequence Numbers of Prefix List Entries Are Specified

By default, the sequence numbers are automatically generated when you create a prefix list entry. Sequence numbers can be suppressed with the **no ip prefix-list sequence-number** global configuration command. Sequence values are generated in increments of 5. The first sequence value generated in a prefix list would be 5, then 10, then 15, and so on. If you specify a value for an entry and then do not specify values for subsequent entries, the assigned (generated) sequence values are incremented in units of five. For example, if you specify that the first entry in the prefix list has a sequence value of 3, and then do not specify sequence values for the other entries, the automatically generated numbers will be 8, 13, 18, and so on.

To disable the automatic generation of sequence numbers, use the following command in router configuration mode:

Command	Purpose
`Router(config-router)# no ip prefix-list sequence-number`	Disables the automatic generation of the sequence numbers for prefix list entries.

To re-enable automatic generation of the sequence numbers of prefix list entries, use the **ip prefix-list sequence number** command in router configuration mode:

Command	Purpose
`Router(config-router)# ip prefix-list sequence-number`	Enables the automatic generation of the sequence numbers of prefix list entries. The default is enable.

If you disable automatic generation of sequence numbers in a prefix list, you must specify the sequence number for each entry using the *sequence-value* argument of the **ip prefix-list** global configuration command.

Regardless of whether the default sequence numbers are used in configuring a prefix list, a sequence number need not be specified when deconfiguring an entry. **show** commands include the sequence numbers in their output.

Deleting a Prefix List or Prefix List Entries

To delete a prefix list, use the following command in router configuration mode:

Command	Purpose
`Router(config-router)# no ip prefix-list list-name`	Deletes a prefix list.

You can delete entries from a prefix list individually. To delete an entry in a prefix list, use the following command in router configuration mode:

Command	Purpose
`Router(config-router)# no ip prefix-list seq sequence-value`	Deletes an entry in a prefix list.

Note The sequence number of an entry need not be specified when you delete the entry.

Displaying Prefix Entries

To display information about prefix tables, prefix table entries, the policy associated with a node, or specific information about an entry, use the following commands in EXEC mode as needed:

Command	Purpose
`Router# show ip prefix-list [detail | summary]`	Displays information about all prefix lists.
`Router# show ip prefix-list [detail | summary] prefix-list-name`	Displays a table showing the entries in a prefix list.
`Router# show ip prefix-list prefix-list-name [network/length]`	Displays the policy associated with the node.
`Router# show ip prefix-list prefix-list-name [seq sequence-number]`	Displays the prefix list entry with a given sequence number.

`Router# show ip prefix-list prefix-list-name [network/length] longer`	Displays all entries of a prefix list that are more specific than the given network and length.
`Router# show ip prefix-list prefix-list-name [network/length] first-match`	Displays the entry of a prefix list that matches the given prefix (network and length of prefix).

Clearing the Hit Count Table of Prefix List Entries

To clear the hit count table of prefix list entries, use the following command in EXEC mode:

Command	Purpose
`Router# clear ip prefix-list prefix-list-name [network/length]`	Clears the hit count table of the prefix list entries.

Configuring BGP Path Filtering by Neighbor

In addition to filtering routing updates based on network numbers, you can specify an access list filter on both incoming and outbound updates based on the BGP autonomous system paths. Each filter is an access list based on regular expressions. To specify the access list filter, define an autonomous system path access list and apply it to updates to and from particular neighbors. See the "Regular Expressions" appendix in the *Cisco IOS Terminal Services Configuration Guide* for more information on forming regular expressions.

To configure BGP path filtering, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	`Router# ip as-path access-list access-list-number {permit | deny} as-regexp`	Defines a BGP-related access list.
Step 2	`Router# router bgp as-number`	Enters router configuration mode.
Step 3	`Router(config-router)# neighbor {ip-address | peer-group-name} filter-list access-list-number {in | out}`	Establishes a BGP filter.

See the "BGP Path Filtering by Neighbor Examples" section at the end of this chapter for an example of BGP path filtering by neighbor.

Disabling Next Hop Processing on BGP Updates

You can configure the Cisco IOS software to disable next hop processing for BGP updates to a neighbor. Disabling next hop processing might be useful in nonmeshed networks such as Frame Relay or X.25, where BGP neighbors might not have direct access to all other neighbors on the same IP subnet. There are two ways to disable next hop processing:

- Provide a specific address to be used instead of the next hop address (manually configuring each address).
- Use a route map to specify that the address of the remote peer for matching inbound routes, or the local router for matching outbound routes (automatic method).

Disabling Next Hop Processing Using a Specific Address

To disable next hop processing and provide a specific address to be used instead of the next hop address, use the following command in router configuration mode:

Command	Purpose
`Router(config-router)# neighbor {ip-address | peer-group-name} next-hop-self`	Disables next hop processing on BGP updates to a neighbor.

Configuring this command causes the current router to advertise its peering address as the next hop for the specified neighbor. Therefore, other BGP neighbors will forward to it packets for that address. This configuration is useful in a nonmeshed environment because you know that a path exists from the present router to that address. In a fully meshed environment, this configuration is not useful because it will result in unnecessary extra hops and because there might be a direct access through the fully meshed cloud with fewer hops.

Disabling Next Hop Processing Using a Route Map

To override the inbound next hop setting for BGP routes and specify that the next hop of the matching routes is to be the IP address of the remote peer, or to set the peering address of the local router to be the next hop of the matching routes, use the **neighbor next-hop-self** router configuration command.

To configure the neighbor peering address to be used for the next hop address, use the following command in route map configuration mode:

Command	Purpose
`Router(config-route-map)# set ip next-hop ip-address [...ip-address] [peer-address]`	In an inbound route map of a BGP peer, sets the next hop of the matching routes to be the neighbor peering address, overriding any third-party next hops and allowing the same route map to be applied to multiple BGP peers to override third-party next hops. With an outbound route map of a BGP peer, sets the next hop of the received address to the peering address of the local router, disabling the next hop calculation. The next hop must be an adjacent router.

Configuring the BGP Version

By default, BGP sessions begin using BGP Version 4 and negotiating downward to earlier versions if necessary. To prevent negotiation and force the BGP version used to communicate with a neighbor, use the following command in router configuration mode:

Command	Purpose
`Router(config-router)# neighbor {ip-address | peer-group-name} version number`	Specifies the BGP version to use when communicating with a neighbor.

Configuring the MED Metric

BGP uses the MED metric as a hint to external neighbors about preferred paths. (The name of this metric for BGP Versions 2 and 3 is INTER_AS_METRIC.) To set the MED of the redistributed routes, Use the following command in router configuration mode. All the routes without a MED will also be set to this value.

Command	Purpose
`Router(config-router)# default-metric number`	Sets an MED.

Alternatively, you can set the MED using the **route-map** router configuration command. See the "BGP Route Map Examples" section at the end of this chapter for examples of using BGP route maps.

Configuring Advanced BGP Features

The tasks in this section are for configuring advanced BGP features.

Using Route Maps to Modify Updates

You can use a route map on a per-neighbor basis to filter updates and modify various attributes. A route map can be applied to either inbound or outbound updates. Only the routes that pass the route map are sent or accepted in updates.

On both the inbound and the outbound updates, we support matching based on autonomous system path, community, and network numbers. Autonomous system path matching requires the **as-path access-list** global configuration command, community based matching requires the **ip community-list** global configuration command and network-based matching requires the **ip access-list** global configuration command. To apply a route map to incoming and outgoing routes, use the following command in router configuration mode:

Command	Purpose
`outer(config-router)# neighbor {ip-address | peer-group-name} route-map map-name {in | out}`	Applies a route map to incoming or outgoing routes.

See the "BGP Route Map Examples" section at the end of this chapter for BGP route map examples.

Resetting eBGP Connections Immediately upon Link Failure

Normally, when a link between external neighbors goes down, the BGP session will not be reset immediately.To reset the eBGP session as soon as an interface goes down, use the following command in router configuration mode:

Command	Purpose
`Router(config-router)# bgp fast-external-fallover`	Resets eBGP sessions automatically.

Configuring Aggregate Addresses

CIDR enables you to create aggregate routes (or *supernets*) to minimize the size of routing tables. You can configure aggregate routes in BGP either by redistributing an aggregate route into BGP or by using the BGP Conditional Aggregation feature. An aggregate address will be added to the BGP table if at least one more specific entry is in the BGP table.

To create an aggregate address in the routing table, use the following commands in router configuration mode:

Command	Purpose
`Router(config-router)# aggregate-address address mask`	Creates an aggregate entry in the BGP routing table.
`Router(config-router)# aggregate-address address mask as-set`	Generates autonomous system set path information.
`Router(config-router)# aggregate-address address-mask summary-only`	Advertises summary addresses only.
`Router(config-router)# aggregate-address address mask suppress-map map-name`	Suppresses selected, more specific routes.
`Router(config-router)# aggregate-address address mask advertise-map map-name`	Generates an aggregate based on conditions specified by the route map.
`Router(config-router)# aggregate-address address mask attribute-map map-name`	Generates an aggregate with attributes specified in the route map.

See the "BGP Aggregate Route Examples" section at the end of this chapter for examples of using BGP aggregate routes.

Disabling Automatic Summarization of Network Numbers

In BGP Version 3, when a subnet is redistributed from an IGP into BGP, only the network route is injected into the BGP table. By default, this automatic summarization is enabled. To disable automatic network number summarization, use the following command in router configuration mode:

Command	Purpose
`Router(config-router)# no auto-summary`	Disables automatic network summarization.

Configuring BGP Community Filtering

BGP supports transit policies via controlled distribution of routing information. The distribution of routing information is based on one of the following three values:

- IP address (see the "Configuring BGP Route Filtering by Neighbor" section earlier in this chapter).
- The value of the autonomous system path attribute (see the "Configuring BGP Path Filtering by Neighbor" section earlier in this chapter).
- The value of the communities attribute (as described in this section).

The *communities* attribute is a way to group destinations into communities and apply routing decisions based on the communities. This method simplifies the configuration of a BGP speaker that controls distribution of routing information.

A *community* is a group of destinations that share some common attribute. Each destination can belong to multiple communities. Autonomous system administrators can define to which communities a destination belongs. By default, all destinations belong to the general Internet community. The community is carried as the communities attribute.

The communities attribute is an optional, transitive, global attribute in the numerical range from 1 to 4,294,967,200. Along with Internet community, there are a few predefined, well-known communities, as follows:

- internet—Advertise this route to the Internet community. All routers belong to it.
- no-export—Do not advertise this route to eBGP peers.
- no-advertise—Do not advertise this route to any peer (internal or external).
- local-as—Do not advertise this route to peers outside the local autonomous system. This route will not be advertised to other autonomous systems or sub-autonomous systems when confederations are configured.

Based on the community, you can control which routing information to accept, prefer, or distribute to other neighbors. A BGP speaker can set, append, or modify the community of a route when you learn, advertise, or redistribute routes. When routes are aggregated, the resulting aggregate has a communities attribute that contains all communities from all the initial routes.

You can use community lists to create groups of communities to use in a match clause of a route map. Just like an access list, a series of community lists can be created. Statements are checked until a match is found. As soon as one statement is satisfied, the test is concluded.

To create a community list, use the following command in global configuration mode:

Command	Purpose
`Router(config)# ip community-list community-list-number {permit | deny} community-number`	Creates a community list.

To set the communities attribute and match clauses based on communities, see the **match community-list** and **set community** route map configuration commands in the "Redistribute Routing Information" section in the "Configuring IP Routing Protocol-Independent Features" chapter.

By default, no communities attribute is sent to a neighbor. To specify that the communities attribute to be sent to the neighbor at an IP address, use the following command in router configuration mode:

Command	Purpose
`Router(config-router)# neighbor {ip-address | peer-group-name} send-community [both | standard | extended]`	Specifies that the communities attribute be sent to the neighbor at this IP address. Both standard and extended communities can be specified with the **both** keyword. Only standard or only extended can be specified with the **standard** and **extended** keywords.

To remove communities from the community attribute of an inbound or outbound update using a route map to filter and determine the communities to be deleted, use the following command in router configuration mode:

Command	Purpose
`Router(config-router)# set comm-list` *community-list-number* `delete`	Removes communities in a community attribute that match a standard or extended community list.

Specifying the Format for the Community

A BGP community is displayed in a two-part format 2 bytes long in the **show ip bgp community** EXEC command output, and wherever communities are displayed in the router configuration, such as router maps and community lists. In the most recent version of the RFC for BGP, a community is of the form AA:NN, where the first part is the autonomous system number and the second part is a 2-byte number. The Cisco default community format is in the format NNAA.

To display BGP communities in the new format, use the following command in global configuration mode:

Command	Purpose
`Router(config)# ip bgp-community new-format`	Displays and parses BGP communities in the format AA:NN.

Configuring BGP Conditional Advertisement

BGP advertises routes from its routing table to external peers (peers in different autonomous systems) by default. The BGP Conditional Advertisement feature provides additional control of route advertisement depending on the existence of other prefixes in the BGP table. Normally, routes are propagated regardless of the existence of a different path. The BGP Conditional Advertisement feature uses the non-exist-map and the advertise-map to track routes by the route prefix. If a route prefix is not present in the non-exist-map, the route specified by the advertise-map is announced. The announced route is installed to the BGP routing table as a locally originated route and will behave as a locally originated route. The announced route will be originated by BGP only if the corresponding IGP route exists. After the prefix is locally originated by BGP, BGP will advertise the prefix to internal and external peers. If the route prefix is present, the route in the advertise-map is not announced.

Conditional advertisement can be useful in a multihomed network, in which some prefixes are to be advertised to one of the providers, only if information from the other provider is missing. This condition would indicate a failure in the peering session, or partial reachability.

If the same information is advertised to all providers in a multihomed environment, the information is duplicated in the global BGP table. When the BGP Conditional Advertisement feature is used, only partial routes are advertised to each provider, and the size of the global BGP table is not increased with redundant information. The administrator can also guarantee the path that inbound traffic will follow because only specific paths are advertised to providers.

Note The conditional BGP announcements are sent in addition to the normal announcements that a BGP router sends to its peers.

Note Autonomous system path list information cannot be used for conditional advertisement because the IP routing table does not contain autonomous system path information.

BGP Conditional Advertisement Configuration Task List

See the following section for configuration tasks for the BGP Conditional Advertisement feature. Each task in the list indicates if the task is optional or required.

- Configure the route-maps that will be used in conjunction with the advertise-map and the non-exist-map. This step may include the configuration of access-lists and prefix-lists. (Required)
- Configure the router to run BGP. (Required)
- Configure the advertise-map and the non-exist-map with the **neighbor advertise-map non-exist-map** router configuration command. (Required)
- Verify that the BGP Condition Advertisement feature has been configured with the **show ip bgp neighbor** command. (Optional)

Conditional Advertisement of a Set of Routes

To conditionally advertise a set of routes, use the following commands beginning in router configuration mode:

	Command	Purpose
Step 1	`Router(config)# router bgp as-number`	Configures the router to run a BGP process.
Step 2	`Router(config-router)# neighbor ip-address remote-as as-number`	Specifies the peer that should receive conditional advertisement for a given set routes.
Step 3	`Router(config-router)# neighbor ip-address advertise-map map1 non-exist-map map2`	Configures the advertise-map and non-exist map for the BGP Conditional Advertisement feature.

See the "BGP Conditional Advertisement Configuration Examples" section at the end of this chapter for an example configuration of BGP conditional advertisement.

Verifying BGP Conditional Advertisement

To verify that the BGP Condition Advertisement feature has been configured, use the **show ip bgp neighbor** command. The **show ip bgp neighbor EXEC** command will show the status of the BGP Conditional Advertisement feature as initialized or uninitialized. The following example shows output from the **show ip bgp neighbor EXEC** command:

```
router# show ip bgp neigbor 172.16.1.1
BGP neighbor is 172.16.1.1,  remote AS 65200, internal link
 Description:link to boston as 65200
  BGP version 4, remote router ID 10.1.1.1
  BGP state = Established, up for 01:04:30
  Last read 00:00:30, hold time is 180, keepalive interval is 60 seconds
  Neighbor capabilities:
    Route refresh:advertised and received
    Address family IPv4 Unicast:advertised and received
  Received 83 messages, 0 notifications, 0 in queue
  Sent 78 messages, 0 notifications, 0 in queue
```

```
  Route refresh request:received 0, sent 0
  Minimum time between advertisement runs is 5 seconds

 For address family:IPv4 Unicast
  BGP table version 18, neighbor version 18
  Index 2, Offset 0, Mask 0x4
  Inbound soft reconfiguration allowed
  NEXT_HOP is always this router
  Community attribute sent to this neighbor
  Condition-map old-route, Advertise-map new-route, status:Uninitialized
  2 accepted prefixes consume 72 bytes
  Prefix advertised 7, suppressed 0, withdrawn 4

  Connections established 1; dropped 0
  Last reset 01:05:29, due to Soft reconfig change
```

BGP Conditional Advertisement Troubleshooting Tips

This section provides troubleshooting information for the BGP conditional advertisement feature.

The BGP Conditional Advertisement feature is based on the nonexistence of a prefix and the advertisement of another. Normally, only two problems can occur:

- The tracked prefix exists, but the conditional advertisement occurs.
- The tracked prefix does not exist, and the conditional advertisement does not occur.

The same method of troubleshooting is used for both problems:

- Verify the existence (or not) of the tracked prefix in the BGP table with the **show ip bgp EXEC** command.
- Verify the advertisement (or not) of the other prefix using the **show ip bgp neighbor advertised-routes EXEC** command.

The user needs to ensure that all of the characteristics specified in the route maps match the routes in the BGP table.

Configuring a Routing Domain Confederation

One way to reduce the iBGP mesh is to divide an autonomous system into multiple subautonomous systems and group them into a single confederation. To the outside world, the confederation looks like a single autonomous system. Each autonomous system is fully meshed within itself, and has a few connections to other autonomous systems in the same confederation. Even though the peers in different autonomous systems have eBGP sessions, they exchange routing information as if they were iBGP peers. Specifically, the next hop, MED, and local preference information is preserved. This feature allows the you to retain a single IGP for all of the autonomous systems.

To configure a BGP confederation, you must specify a confederation identifier. To the outside world, the group of autonomous systems will look like a single autonomous system with the confederation identifier as the autonomous system number. To configure a BGP confederation identifier, use the following command in router configuration mode:

Command	Purpose
`Router(config-router)# bgp confederation identifier` *as-number*	Configures a BGP confederation.

In order to treat the neighbors from other autonomous systems within the confederation as special eBGP peers, use the following command in router configuration mode:

Command	Purpose
`Router(config-router)# bgp confederation peers as-number [as-number]`	Specifies the autonomous systems that belong to the confederation.

See the "BGP Community with Route Maps Examples" section at the end of this chapter for an example configuration of several peers in a confederation.

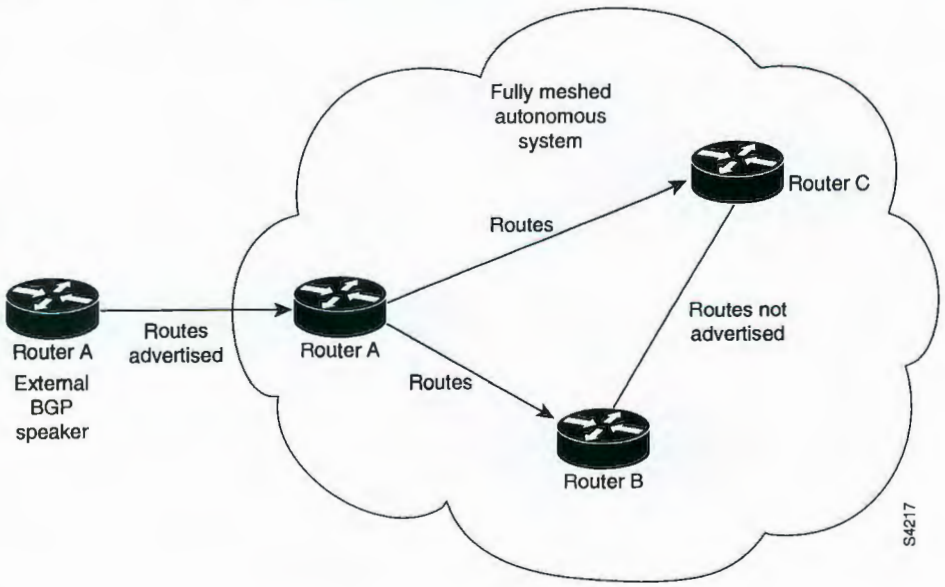
For an alternative way to reduce the iBGP mesh, see the next section, "Configuring a Route Reflector."

Configuring a Route Reflector

BGP requires that all iBGP speakers be fully meshed. However, this requirement does not scale well when there are many iBGP speakers. Instead of configuring a confederation, another way to reduce the iBGP mesh is to configure a *route reflector.*

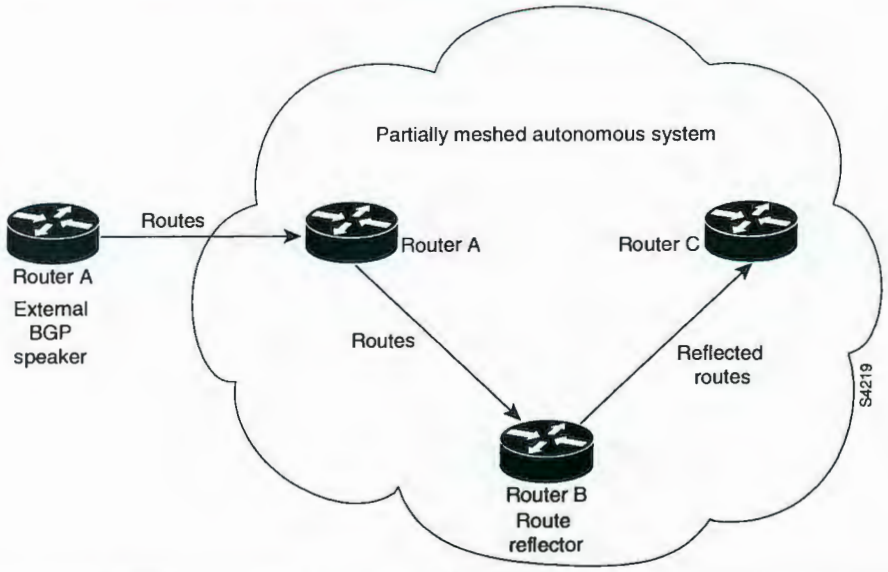
Figure 53 illustrates a simple iBGP configuration with three iBGP speakers (Routers A, B, and C). Without route reflectors, when Router A receives a route from an external neighbor, it must advertise it to both routers B and C. Routers B and C do not readvertise the iBGP learned route to other iBGP speakers because the routers do not pass on routes learned from internal neighbors to other internal neighbors, thus preventing a routing information loop.

Figure 53 Three Fully Meshed iBGP Speakers



With route reflectors, all iBGP speakers need not be fully meshed because there is a method to pass learned routes to neighbors. In this model, an iBGP peer is configured to be a route reflector responsible for passing iBGP learned routes to a set of iBGP neighbors. In Figure 54, Router B is configured as a route reflector. When the route reflector receives routes advertised from Router A, it advertises them to Router C, and vice versa. This scheme eliminates the need for the iBGP session between Routers A and C.

Figure 54 Simple BGP Model with a Route Reflector



The internal peers of the route reflector are divided into two groups: client peers and all the other routers in the autonomous system (nonclient peers). A route reflector reflects routes between these two groups. The route reflector and its client peers form a *cluster*. The nonclient peers must be fully meshed with each other, but the client peers need not be fully meshed. The clients in the cluster do not communicate with iBGP speakers outside their cluster.

Figure 55 More Complex BGP Route Reflector Model

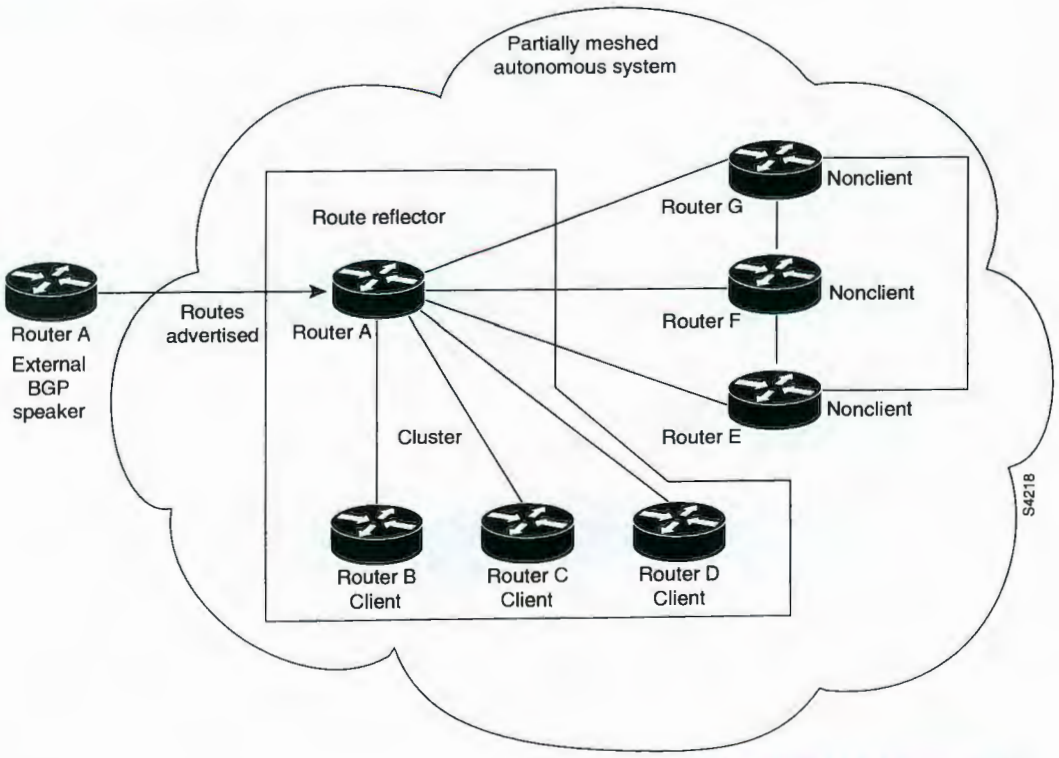


Figure 55 illustrates a more complex route reflector scheme. Router A is the route reflector in a cluster with routers B, C, and D. Routers E, F, and G are fully meshed, nonclient routers.

When the route reflector receives an advertised route, depending on the neighbor, it takes the following actions:

- A route from an external BGP speaker is advertised to all clients and nonclient peers.
- A route from a nonclient peer is advertised to all clients.
- A route from a client is advertised to all clients and nonclient peers. Hence, the clients need not be fully meshed.

To configure a route reflector and its clients, use the following command in router configuration mode:

Command	Purpose
`Router(config-router)# neighbor ip-address | peer-group-name route-reflector-client`	Configures the local router as a BGP route reflector and the specified neighbor as a client.

Along with route reflector-aware BGP speakers, it is possible to have BGP speakers that do not understand the concept of route reflectors. They can be members of either client or nonclient groups allowing a easy and gradual migration from the old BGP model to the route reflector model. Initially, you could create a single cluster with a route reflector and a few clients. All the other iBGP speakers could be nonclient peers to the route reflector and then more clusters could be created gradually.

An autonomous system can have multiple route reflectors. A route reflector treats other route reflectors just like other iBGP speakers. A route reflector can be configured to have other route reflectors in a client group or nonclient group. In a simple configuration, the backbone could be divided into many clusters. Each route reflector would be configured with other route reflectors as nonclient peers (thus, all the route reflectors will be fully meshed). The clients are configured to maintain iBGP sessions with only the route reflector in their cluster.

Usually a cluster of clients will have a single route reflector. In that case, the cluster is identified by the router ID of the route reflector. To increase redundancy and avoid a single point of failure, a cluster might have more than one route reflector. In this case, all route reflectors in the cluster must be configured with the 4-byte cluster ID so that a route reflector can recognize updates from route reflectors in the same cluster. All the route reflectors serving a cluster should be fully meshed and all of them should have identical sets of client and nonclient peers.

If the cluster has more than one route reflector, configure the cluster ID by using the following command in router configuration mode:

Command	Purpose
`Router(config-router)# bgp cluster-id cluster-id`	Configures the cluster ID.

Use the **show ip bgp** EXEC command to display the originator ID and the cluster-list attributes.

By default, the clients of a route reflector are not required to be fully meshed and the routes from a client are reflected to other clients. However, if the clients are fully meshed, the route reflector need not reflect routes to clients.

To disable client-to-client route reflection, use the **no bgp client-to-client reflection** command in router configuration mode:

Command	Purpose
`Router(config-router)# no bgp client-to-client reflection`	Disables client-to-client route reflection.

As the iBGP learned routes are reflected, routing information may loop. The route reflector model has the following mechanisms to avoid routing loops:

- Originator ID is an optional, nontransitive BGP attribute. It is a 4-byte attributed created by a route reflector. The attribute carries the router ID of the originator of the route in the local autonomous system. Therefore, if a misconfiguration causes routing information to come back to the originator, the information is ignored.
- Cluster-list is an optional, nontransitive BGP attribute. It is a sequence of cluster IDs that the route has passed. When a route reflector reflects a route from its clients to nonclient peers, and vice versa, it appends the local cluster ID to the cluster-list. If the cluster-list is empty, a new cluster-list is created. Using this attribute, a route reflector can identify if routing information is looped back to the same cluster due to misconfiguration. If the local cluster ID is found in the cluster-list, the advertisement is ignored.
- Use **set** clauses in outbound route maps to modify attributes, possibly creating routing loops. To avoid this behavior, **set** clauses of outbound route maps are ignored for routes reflected to iBGP peers.

Configuring BGP Peer Groups

Often, in a BGP speaker, many neighbors are configured with the same update policies (that is, the same outbound route maps, distribute lists, filter lists, update source, and so on). Neighbors with the same update policies can be grouped into peer groups to simplify configuration and, more importantly, to make updating more efficient. When you have many peers, this approach is highly recommended.

The three steps to configure a BGP peer group, described in the following sections, are as follows:

1. Creating the Peer Group
2. Assigning Options to the Peer Group
3. Making Neighbors Members of the Peer Group

You can disable a BGP peer or peer group without removing all the configuration information using the **neighbor shutdown** router configuration command.

Creating the Peer Group

To create a BGP peer group, use the following command in router configuration mode:

Command	Purpose
`Router(config-router)# neighbor peer-group-name peer-group`	Creates a BGP peer group.

Assigning Options to the Peer Group

After you create a peer group, you configure the peer group with **neighbor** commands. By default, members of the peer group inherit all the configuration options of the peer group. Members can also be configured to override the options that do not affect outbound updates.

Peer group members will always inherit the following attributes: minimum-advertisement-interval, next-hop-self, out-route-map, out-filter-list, out-dist-list, remote-as (if configured), version, and update-source. All the peer group members will inherit changes made to the peer group.

To assign configuration options to an individual neighbor, specify any of the following commands using the IP address. To assign the options to a peer group, specify any of the commands using the peer group name. Use the following commands in router configuration mode as needed.

Command	Purpose
Router(config-router)# **neighbor** {*ip-address* | *peer-group-name*} **remote-as** *as-number*	Specifies a BGP neighbor.
Router(config-router)# **neighbor** {*ip-address* | *peer-group-name*} **description** *text*	Associates a description with a neighbor.
Router(config-router)# **neighbor** {*ip-address* | *peer-group-name*} **default-originate** [**route-map** *map-name*]	Allows a BGP speaker (the local router) to send the default route 0.0.0.0 to a neighbor for use as a default route.
Router(config-router)# **neighbor** {*ip-address* | *peer-group-name*} **send-community**	Specifies that the communities attribute be sent to the neighbor at this IP address.
Router(config-router)# **neighbor** {*ip-address* | *peer-group-name*} **update-source** *interface-type*	Allows iBGP sessions to use any operational interface for TCP connections.
Router(config-router)# **neighbor** {*ip-address* | *peer-group-name*} **ebgp-multihop**	Allows BGP sessions, even when the neighbor is not on a directly connected segment. The multihop session is not established if the only route to the address of the multihop peer is the default route (0.0.0.0).
Router(config-router)# **neighbor** {*ip-address* | *peer-group-name*} **advertisement-interval** *seconds*	Sets the minimum interval between sending BGP routing updates.
Router(config-router)# **neighbor** {*ip-address* | *peer-group-name*} **maximum-prefix** *maximum* [*threshold*] [**warning-only**]	Limits the number of prefixes allowed from a neighbor.
Router(config-router)# **neighbor** {*ip-address* | *peer-group-name*} **password** *string*	Invokes MD5 authentication on a TCP connection to a BGP peer.
Router(config-router)# **neighbor** {*ip-address* | *peer-group-name*} **distribute-list** {*access-list-number* | *access-list-name*} {**in** | **out**}	Filters BGP routing updates to and from neighbors, as specified in an access list.
Router(config-router)# **neighbor** {*ip-address* | *peer-group-name*} **filter-list** *access-list-number* {**in** | **out**}	Establishes a BGP filter.
Router(config-router)# **neighbor** {*ip-address* | *peer-group-name*} **next-hop-self**	Disables next hop processing on the BGP updates to a neighbor.
Router(config-router)# **neighbor** {*ip-address* | *peer-group-name*} **version** *value*	Specifies the BGP version to use when communicating with a neighbor.

Command	Purpose
`Router(config-router)# neighbor {ip-address | peer-group-name} route-map map-name {in | out}`	Applies a route map to incoming or outgoing routes.
`Router(config-router)# neighbor {ip-address | peer-group-name} soft-reconfiguration inbound`	Configures the software to start storing received updates. This command requires at least one keyword. Currently the only keyword available is **inbound**, so the use of inbound is not optional.

If a peer group is not configured with a remote-as attribute, the members can be configured with the **neighbor remote-as** router configuration command. This command allows you to create peer groups containing eBGP neighbors.

You can customize inbound policies for peer group members (using, for example, a distribute list, route map, or filter list) because one identical copy of an update is sent to every member of a group. Therefore, neighbor options related to outgoing updates cannot be customized for peer group members.

External BGP peers normally must reside on a directly connected network. Sometimes it is useful to relax this restriction in order to test BGP; do so by specifying the **neighbor ebgp-multihop** router configuration command.

Note To avoid the accidental creation of loops through oscillating routes, the multihop session will not be established if the only route to the address of the multihop peer is the default route (0.0.0.0).

Members of a peer group can pass routes from one member of the peer group to another. For example, if router B is peering with routers A and C, router B can pass routes from router A to router C.

For iBGP, you might want to allow your BGP connections to stay up regardless of which interface is used to reach a neighbor. To enable this configuration, you first configure a *loopback* interface and assign it an IP address. Next, configure the BGP update source to be the loopback interface. Finally, configure your neighbor to use the address on the loopback interface. Now the iBGP session will be up as long as there is a route, regardless of any interface.

You can set the minimum interval of time between BGP routing updates.

You can invoke MD5 authentication between two BGP peers, meaning that each segment sent on the TCP connection between them is verified. This feature must be configured with the same password on both BGP peers; otherwise, the connection between them will not be made. The authentication feature uses the MD5 algorithm. Invoking authentication causes the Cisco IOS software to generate and check the MD5 digest of every segment sent on the TCP connection. If authentication is invoked and a segment fails authentication, then a message appears on the console.

See the "BGP Peer Group Examples" at the end of this chapter for an example of enabling MD5 authentication.

Making Neighbors Members of the Peer Group

To configure a BGP neighbor to be a member of a BGP peer group, use the following command in router configuration mode, using the same peer group name:

Command	Purpose
`Router(config-router)# neighbor ip-address peer-group peer-group-name`	Makes a BGP neighbor a member of the peer group.

See the "BGP Peer Group Examples" section at the end of this chapter for examples of iBGP and eBGP peer groups.

Disabling a Peer or Peer Group

To disable an existing BGP neighbor or neighbor peer group, use the following command in router configuration mode:

Command	Purpose
`Router(config-router)# neighbor {ip-address | peer-group-name} shutdown`	Shuts down or disables a BGP neighbor or peer group.

To enable a previously existing neighbor or neighbor peer group that had been disabled using the **neighbor shutdown** router configuration command, use the following command in router configuration mode:

Command	Purpose
`Router(config-router)# no neighbor {ip-address | peer-group-name} shutdown`	Enables a BGP neighbor or peer group.

Indicating Backdoor Routes

You can indicate which networks are reachable by using a *backdoor* route that the border router should use. A backdoor network is treated as a local network, except that it is not advertised. To configure backdoor routes, use the **network backdoor** command, beginning in router configuration mode:

Command	Purpose
`Router(config-router)# network ip-address backdoor`	Indicates reachable networks through backdoor routes.

Modifying Parameters While Updating the IP Routing Table

By default, when a BGP route is put into the IP routing table, the MED is converted to an IP route metric, the BGP next hop is used as the next hop for the IP route, and the tag is not set. However, you can use a route map to perform mapping. To modify metric and tag information when the IP routing table is updated with BGP learned routes, use the following command in router configuration mode:

Command	Purpose
`Router(config-router)# table-map map-name`	Applies a route map to routes when updating the IP routing table.

Setting Administrative Distance

Administrative distance is a measure of the preference of different routing protocols. BGP uses three different administrative distances: external, internal, and local. Routes learned through external BGP are given the external distance, routes learned with iBGP are given the internal distance, and routes that are part of this autonomous system are given the local distance. To assign a BGP administrative distance, use the following command in router configuration mode:

Command	Purpose
`Router(config-router)# distance bgp external-distance internal-distance local-distance`	Assigns a BGP administrative distance.

Changing the administrative distance of BGP routes is considered dangerous and generally is not recommended. The external distance should be lower than any other dynamic routing protocol, and the internal and local distances should be higher than any other dynamic routing protocol.

Adjusting BGP Timers

BGP uses certain timers to control periodic activities such as the sending of keepalive messages and the interval after not receiving a keepalive message after which the Cisco IOS software declares a peer dead. By default, the keepalive timer is 60 seconds, and the hold-time timer is 180 seconds.You can adjust these timers. When a connection is started, BGP will negotiate the hold time with the neighbor. The smaller of the two hold times will be chosen. The keepalive timer is then set based on the negotiated hold time and the configured keepalive time.

To adjust BGP timers for all neighbors, use the following command in router configuration mode:

Command	Purpose
`Router(config-router)# timers bgp keepalive holdtime`	Adjusts BGP timers for all neighbors.

To adjust BTP keepalive and hold-time timers for a specific neighbor, use the following command in router configuration mode:

Command	Purpose
`Router(config-router)# neighbor [ip-address | peer-group-name] timers keepalive holdtime`	Sets the keepalive and hold-time timers (in seconds) for the specified peer or peer group.

Note The timers configured for a specific neighbor or peer group override the timers configured for all BGP neighbors using the **timers bgp** router configuration command.

To clear the timers for a BGP neighbor or peer group, use the **no** form of the **neighbor timers** command.

Changing the Default Local Preference Value

You can define a particular path as more preferable or less preferable than other paths by changing the default local preference value of 100. To assign a different default local preference value, use the following command in router configuration mode:

Command	Purpose
`Router(config-router)# bgp default local-preference` *value*	Changes the default local preference value.

You can use route maps to change the default local preference of specific paths. See the "BGP Route Map Examples" section at the end of this chapter for examples when used with BGP route maps.

Redistributing Network 0.0.0.0

By default, you are not allowed to redistribute network 0.0.0.0. To permit the redistribution of network 0.0.0.0, use the following command in router configuration mode:

Command	Purpose
`Router(config-router)# default-information originate`	Allows the redistribution of network 0.0.0.0 into BGP.

Configuring the Router to Consider a Missing MED as Worst Path

To configure the router to consider a path with a missing MED attribute as the worst path, use the following command in router configuration mode:

Command	Purpose
`Router(config-router)# bgp bestpath med missing-as-worst`	Configures the router to consider a missing MED as having a value of infinity, making the path without a MED value the least desirable path.

Selecting Path Based on MEDs from Other Autonomous Systems

The MED is one of the parameters that is considered when selecting the best path among many alternative paths. The path with a lower MED is preferred over a path with a higher MED.

By default, during the best path selection process, MED comparison is done only among paths from the same autonomous system. You can allow comparison of MEDs among paths regardless of the autonomous system from which the paths are received. To do so, use the following command in router configuration mode:

Command	Purpose
`Router(config-router)# bgp always-compare-med`	Allows the comparison of MEDs for paths from neighbors in different autonomous systems.

Configuring the Router to Use the MED to Choose a Path from Subautonomous System Paths

To configure the router to consider the MED value in choosing a path, use the following command in router configuration mode:

Command	Purpose
`Router(config-router)# bgp bestpath med confed`	Configures the router to consider the MED in choosing a path from among those advertised by different subautonomous systems within a confederation.

The comparison between MEDs is only made if there are no external autonomous systems in the path (an external autonomous system is an autonomous system that is not within the confederation). If there is an external autonomous system in the path, then the external MED is passed transparently through the confederation, and the comparison is not made.

The following example compares route A with these paths:

```
path= 65000 65004, med=2
path= 65001 65004, med=3
path= 65002 65004, med=4
path= 65003 1, med=1
```

In this case, path 1 would be chosen if the **bgp bestpath med confed** router configuration command is enabled. The fourth path has a lower MED, but it is not involved in the MED comparison because there is an external autonomous system is in this path.

Configuring the Router to Use the MED to Choose a Path in a Confederation

To configure the router to use the MED to select the best path from among paths advertised by a single subautonomous system within a confederation, use the following command in router configuration mode:

Command	Purpose
`Router(config-router)# bgp deterministic med`	Configures the router to compare the MED variable when choosing among routes advertised by different peers in the same autonomous system.

Note If the **bgp always-compare-med** router configuration command is enabled, all paths are fully comparable, including those from other autonomous systems in the confederation, even if the **bgp deterministic med** command is also enabled.

Configuring Route Dampening

Route dampening is a BGP feature designed to minimize the propagation of flapping routes across an internetwork. A route is considered to be flapping when it is repeatedly available, then unavailable, then available, then unavailable, and so on.

For example, consider a network with three BGP autonomous systems: autonomous system 1, autonomous system 2, and autonomous system 3. Suppose the route to network A in autonomous system 1 flaps (it becomes unavailable). Under circumstances without route dampening, the eBGP neighbor of autonomous system 1 to autonomous system 2 sends a withdraw message to autonomous system 2. The border router in autonomous system 2, in turn, propagates the withdraw message to autonomous system 3. When the route to network A reappears, autonomous system 1 sends an advertisement message to autonomous system 2, which sends it to autonomous system 3. If the route to network A repeatedly becomes unavailable, then available, many withdrawal and advertisement messages are sent. This is a problem in an internetwork connected to the Internet because a route flap in the Internet backbone usually involves many routes.

Note No penalty is applied to a BGP peer reset when route dampening is enabled. Although the reset withdraws the route, no penalty is applied in this instance, even if route flap dampening is enabled.

Minimizing Flapping

The route dampening feature minimizes the flapping problem as follows. Suppose again that the route to network A flaps. The router in autonomous system 2 (where route dampening is enabled) assigns network A a penalty of 1000 and moves it to history state. The router in autonomous system 2 continues to advertise the status of the route to neighbors. The penalties are cumulative. When the route flaps so often that the penalty exceeds a configurable suppress limit, the router stops advertising the route to network A, regardless of how many times it flaps. Thus, the route is dampened.

The penalty placed on network A is decayed until the reuse limit is reached, upon which the route is once again advertised. At half of the reuse limit, the dampening information for the route to network A is removed.

Understanding Route Dampening Terms

The following terms are used when describing route dampening:

- Flap—A route is available, then unavailable, or vice versa.
- History state—After a route flaps once, it is assigned a penalty and put into history state, meaning the router does not have the best path, based on historical information.
- Penalty—Each time a route flaps, the router configured for route dampening in another autonomous system assigns the route a penalty of 1000. Penalties are cumulative. The penalty for the route is stored in the BGP routing table until the penalty exceeds the suppress limit. At that point, the route state changes from history to damp.
- Damp state—In this state, the route has flapped so often that the router will not advertise this route to BGP neighbors.
- Suppress limit—A route is suppressed when its penalty exceeds this limit. The default value is 2000.
- Half-life—Once the route has been assigned a penalty, the penalty is decreased by half after the half-life period (which is 15 minutes by default). The process of reducing the penalty happens every 5 seconds.

- Reuse limit—As the penalty for a flapping route decreases and falls below this reuse limit, the route is unsuppressed. That is, the route is added back to the BGP table and once again used for forwarding. The default reuse limit is 750. The process of unsuppressing routes occurs at 10-second increments. Every 10 seconds, the router finds out which routes are now unsuppressed and advertises them to the world.
- Maximum suppress limit—This value is the maximum amount of time a route can be suppressed. The default value is four times the half-life.

The routes external to an autonomous system learned via iBGP are not dampened. This policy prevent the iBGP peers from having a higher penalty for routes external to the autonomous system.

Enabling Route Dampening

To enable BGP route dampening, use the following command in address family or router configuration mode:

Command	Purpose
`Router(config)# bgp dampening`	Enables BGP route dampening.

To change the default values of various dampening factors, use the following command in address family or router configuration mode:

Command	Purpose
`Router(config)# bgp dampening` *half-life reuse suppress max-suppress* [`route-map` *map-name*]	Changes the default values of route dampening factors.

Monitoring and Maintaining BGP Route Dampening

You can monitor the flaps of all the paths that are flapping. The statistics will be deleted once the route is not suppressed and is stable for at least one half-life. To display flap statistics, use the following commands in EXEC mode as needed:

Command	Purpose
`Router# show ip bgp flap-statistics`	Displays BGP flap statistics for all paths.
`Router# show ip bgp flap-statistics regexp` *regexp*	Displays BGP flap statistics for all paths that match the regular expression.
`Router# show ip bgp flap-statistics filter-list` *access-list*	Displays BGP flap statistics for all paths that pass the filter.
`Router# show ip bgp flap-statistics` *ip-address mask*	Displays BGP flap statistics for a single entry.
`Router# show ip bgp flap-statistics` *ip-address mask* `longer-prefix`	Displays BGP flap statistics for more specific entries.

To clear BGP flap statistics (thus making it less likely that the route will be dampened), use the following commands in EXEC mode as needed:

Command	Purpose
`Router# clear ip bgp flap-statistics`	Clears BGP flap statistics for all routes.
`Router# clear ip bgp flap-statistics regexp regexp`	Clears BGP flap statistics for all paths that match the regular expression.
`Router# clear ip bgp flap-statistics filter-list list`	Clears BGP flap statistics for all paths that pass the filter.
`Router# clear ip bgp flap-statistics ip-address mask`	Clears BGP flap statistics for a single entry.
`Router# clear ip bgp ip-address flap-statistics`	Clears BGP flap statistics for all paths from a neighbor.

Note The flap statistics for a route are also cleared when a BGP peer is reset. Although the reset withdraws the route, there is no penalty applied in this instance, even if route flap dampening is enabled.

Once a route is dampened, you can display BGP route dampening information, including the time remaining before the dampened routes will be unsuppressed. To display the information, use the following command in EXEC mode:

Command	Purpose
`Router# show ip bgp dampened-paths`	Displays the dampened routes, including the time remaining before they will be unsuppressed.

You can clear BGP route dampening information and unsuppress any suppressed routes by using the following command in EXEC mode:

Command	Purpose
`Router# clear ip bgp dampening [ip-address network-mask]`	Clears route dampening information and unsuppresses the suppressed routes.

Monitoring and Maintaining BGP

You can remove all contents of a particular cache, table, or database. You also can display specific statistics. The following sections describe each of these tasks.

Clearing Caches, Tables, and Databases

You can remove all contents of a particular cache, table, or database. Clearing a cache, table, or database can become necessary when the contents of the particular structure have become, or are suspected to be, invalid.

To clear caches, tables, and databases for BGP, use the following commands in EXEC mode, as needed:

Command	Purpose
Router# **clear ip bgp** *neighbor-address*	Resets a particular BGP connection.
Router# **clear ip bgp ***	Resets all BGP connections.
Router# **clear ip bgp peer-group** *tag*	Removes all members of a BGP peer group.

Displaying System and Network Statistics

You can display specific statistics such as the contents of BGP routing tables, caches, and databases. Information provided can be used to determine resource utilization and solve network problems. You can also display information about node reachability and discover the routing path that the packets of your device are taking through the network.

To display various routing statistics, use the following commands in EXEC mode, as needed:

Command	Purpose
Router# **show ip bgp** *prefix*	Displays peer groups and peers not in peer groups to which the prefix has been advertised. Also displays prefix attributes such as the next hop and the local prefix.
Router# **show ip bgp cidr-only**	Displays all BGP routes that contain subnet and supernet network masks.
Router# **show ip bgp community** *community-number* [**exact**]	Displays routes that belong to the specified communities.
Router# **show ip bgp community-list** *community-list-number* [**exact**]	Displays routes that are permitted by the community list.
Router# **show ip bgp filter-list** *access-list-number*	Displays routes that are matched by the specified autonomous system path access list.
Router# **show ip bgp inconsistent-as**	Displays the routes with inconsistent originating autonomous systems.
Router# **show ip bgp regexp** *regexp*	Displays the routes that have an autonomous system path that matches the specified regular expression entered on the command line.
Router# **show ip bgp**	Displays the contents of the BGP routing table.
Router# **show ip bgp neighbors** [*neighbor-address*]	Displays detailed information on the BGP and TCP connections to individual neighbors.
Router# **show ip bgp neighbors** [*address*] [**received-routes** | **routes** | **advertised-routes** | **paths** *regexp* | **dampened-routes**]	Displays routes learned from a particular BGP neighbor.
Router# **show ip bgp paths**	Displays all BGP paths in the database.
Router# **show ip bgp peer-group** [*tag*] [**summary**]	Displays information about BGP peer groups.
Router# **show ip bgp summary**	Displays the status of all BGP connections.

Logging Changes in Neighbor Status

To enable the logging of messages generated when a BGP neighbor resets, comes up, or goes down, use the following command in router configuration mode:

Command	Purpose
`Router(config-router)# bgp log-neighbor-changes`	Logs messages generated when a BGP neighbor goes up or down, or resets

BGP Configuration Examples

The following sections provide BGP configuration examples:

- BGP Route Map Examples
- BGP Neighbor Configuration Examples
- BGP Prefix List Filtering Examples
- BGP Soft Reset Examples
- BGP Synchronization Examples
- BGP Path Filtering by Neighbor Examples
- BGP Aggregate Route Examples
- BGP Community with Route Maps Examples
- BGP Conditional Advertisement Configuration Examples
- BGP Confederation Examples
- BGP Peer Group Examples
- TCP MD5 Authentication for BGP Examples

BGP Route Map Examples

The following example shows how you can use route maps to modify incoming data from a neighbor. Any route received from 140.222.1.1 that matches the filter parameters set in autonomous system access list 200 will have its weight set to 200 and its local preference set to 250, and it will be accepted.

```
router bgp 100
!
 neighbor 140.222.1.1 route-map FIX-WEIGHT in
 neighbor 140.222.1.1 remote-as 1
!
ip as-path access-list 200 permit ^690$
ip as-path access-list 200 permit ^1800
!
route-map FIX-WEIGHT permit 10
 match as-path 200
 set local-preference 250
 set weight200
```

In the following example, the route map named freddy marks all paths originating from autonomous system 690 with an MED metric attribute of 127. The second permit clause is required so that routes not matching autonomous system path list 1 will still be sent to neighbor 1.1.1.1.

```
router bgp 100
 neighbor 1.1.1.1 route-map freddy out
!
ip as-path access-list 1 permit ^690_
ip as-path access-list 2 permit .*
!
route-map freddy permit 10
 match as-path 1
 set metric 127
!
route-map freddy permit 20
 match as-path 2
```

The following example shows how you can use route maps to modify redistributed information from the IP forwarding table:

```
router bgp 100
 redistribute igrp 109 route-map igrp2bgp
!
route-map igrp2bgp
 match ip address 1
 set local-preference 25
 set metric 127
 set weight 30000
 set next-hop 192.92.68.24
 set origin igp
!
access-list 1 permit 131.108.0.0 0.0.255.255
access-list 1 permit 160.89.0.0 0.0.255.255
access-list 1 permit 198.112.0.0 0.0.127.255
```

It is proper behavior to not accept any autonomous system path not matching the **match** clause of the route map. This behavior means that you will not set the metric and the Cisco IOS software will not accept the route. However, you can configure the software to accept autonomous system paths not matched in the **match** clause of the **route-map** router configuration command by using multiple maps of the same name, some without accompanying **set** commands.

```
route-map fnord permit 10
 match as-path 1
 set local-preference 5
!
route-map fnord permit 20
 match as-path 2
```

The following example shows how you can use route maps in a reverse operation to set the route tag (as defined by the BGP/OSPF interaction document, RFC 1403) when exporting routes from BGP into the main IP routing table:

```
router bgp 100
 table-map set_ospf_tag
!
route-map set_ospf_tag
 match as-path 1
 set automatic-tag
!
ip as-path access-list 1 permit .*
```

The following example shows how the route map named set-as-path is applied to outbound updates to the neighbor 200.69.232.70. The route map will prepend the autonomous system path "100 100" to routes that pass access list 1. The second part of the route map is to permit the advertisement of other routes.

```
router bgp 100
 network 171.60.0.0
 network 172.60.0.0
 neighbor 200.69.232.70 remote-as 200
 neighbor 200.69.232.70 route-map set-as-path out
!
route-map set-as-path 10 permit
 match address 1
 set as-path prepend 100 100
!
route-map set-as-path 20 permit
 match address 2
!
access-list 1 permit 171.60.0.0 0.0.255.255
access-list 1 permit 172.60.0.0 0.0.255.255
!
access-list 2 permit 0.0.0.0 255.255.255.255
```

Inbound route maps could perform prefix-based matching and set various parameters of the update. Inbound prefix matching is available in addition to autonomous system path and community list matching. The following example shows how the **set local-preference** route-map configuration command sets the local preference of the inbound prefix 140.10.0.0/16 to 120:

```
!
router bgp 100
 network 131.108.0.0
 neighbor 131.108.1.1 remote-as 200
 neighbor 131.108.1.1 route-map set-local-pref in
!
route-map set-local-pref permit 10
 match ip address 2
 set local preference 120
!
route-map set-local-pref permit 20
!
access-list 2 permit 140.10.0.0 0.0.255.255
access-list 2 deny any
```

The following examples show how to ensure that traffic from one router on a shared LAN will always be passed through a second router, rather than being sent directly to a third router on the same LAN.

Routers A, B, and C connect to the same LAN. Router A peers with router B, and router B peers with router C. Router B sends traffic over the routes of router A to router C, but wants to make sure that all traffic from router C to router A goes through router B, rather than directly from router C to router A over the shared LAN. This configuration can be useful for traffic accounting purposes or to satisfy the peering agreement between router C and router B. You can achieve this configuration by using the **set ip next-hop** route-map configuration command as shown in the following two examples.

Example one applies an inbound route map on the BGP session of router C with router B.

Router A Configuration

```
router bgp 100
 neighbor 1.1.1.2 remote-as 200
```

Router B Configuration

```
router bgp 200
```

```
 neighbor 1.1.1.1 remote-as 100
 neighbor 1.1.1.3 remote-as 300
```

Router C Configuration

```
router bgp 300
 neighbor 1.1.1.2 remote-as 200
 neighbor 1.1.1.2 route-map set-peer-address in

route-map set-peer-address permit 10
 set ip next-hop peer-address
```

The following example applies an outbound route map on the BGP session of router B with router C:

Router A Configuration

```
router bgp 100
 neighbor 1.1.1.2 remote-as 200
```

Router B Configuration

```
router bgp 200
 neighbor 1.1.1.1 remote-as 100
 neighbor 1.1.1.3 remote-as 300
 neighbor 1.1.1.3 route-map set-peer-address out

route-map set-peer-address permit 10
 set ip next-hop peer-address
```

Router C Configuration

```
router bgp 300
 neighbor 1.1.1.2 remote-as 200
```

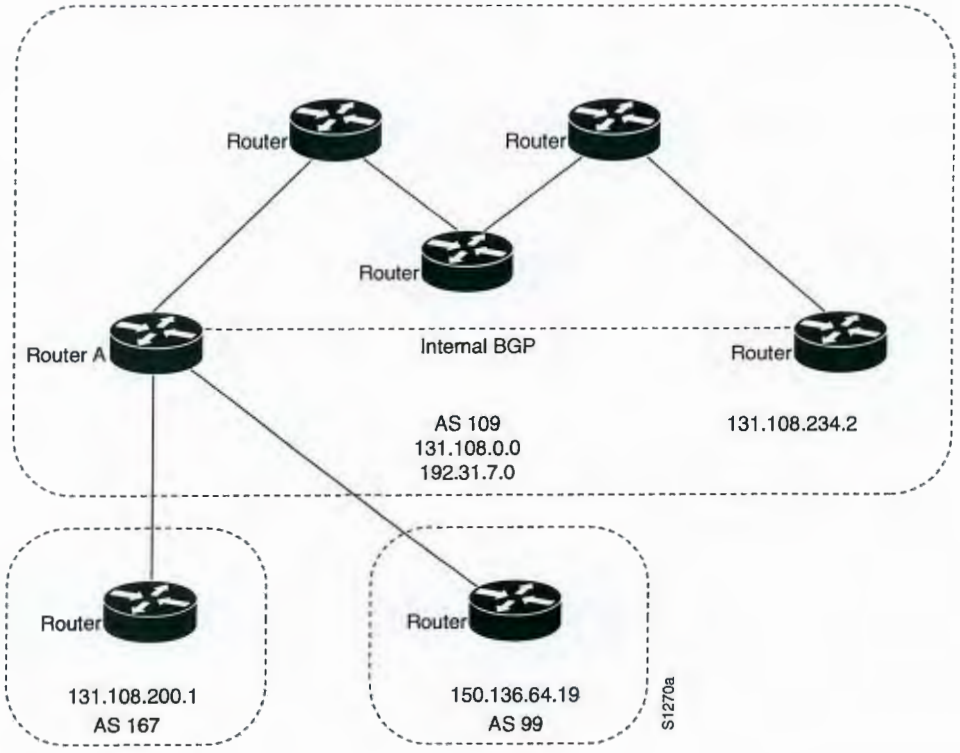
BGP Neighbor Configuration Examples

The following example shows how BGP neighbors on an autonomous system are configured to share information. In the example, a BGP router is assigned to autonomous system 109, and two networks are listed as originating in the autonomous system. Then the addresses of three remote routers (and their autonomous systems) are listed. The router being configured will share information about networks 131.108.0.0 and 192.31.7.0 with the neighbor routers. The first router listed is in a different autonomous system; the second **neighbor remote-as** router configuration command specifies an internal neighbor (with the same autonomous system number) at address 131.108.234.2; and the third **neighbor remote-as** router configuration command specifies a neighbor on a different autonomous system.

```
router bgp 109
 network 131.108.0.0
 network 192.31.7.0
 neighbor 131.108.200.1 remote-as 167
 neighbor 131.108.234.2 remote-as 109
 neighbor 150.136.64.19 remote-as 99
```

In Figure 56, Router A is being configured. The iBGP neighbor is not directly linked to Router A. External neighbors (in autonomous system 167 and autonomous system 99) must be linked directly to Router A.

Figure 56 Assigning Internal and External BGP Neighbors



BGP Prefix List Filtering Examples

The following examples show route filtering using a single prefix list and a group of prefixes, and how to add or delete an individual entry from a prefix list.

Route Filtering Configuration Example Using a Single Prefix List

The following example shows how a prefix list denies the default route 0.0.0.0/0:

```
ip prefix-list abc deny 0.0.0.0/0
```

The following example shows how a prefix list permits a route that matches the prefix 35.0.0.0/8:

```
ip prefix-list abc permit 35.0.0.0/8
```

The following example shows how to configure the BGP process so that it only accept prefixes with a prefix length of /8 to /24:

```
router bgp
version 2
network 101.20.20.0
distribute-list prefix max24 in
!
ip prefix-list max24 seq 5 permit 0.0.0.0/0 ge 8 le 24
```

The following example configuration shows how to conditionally originate a default route (0.0.0.0/0) in RIP when a prefix 10.1.1.0/24 exists in the routing table:

23.321

```
ip prefix-list cond permit 10.1.1.0/24
!
route-map default-condition permit 10
match ip address prefix-list cond
!
router rip
default-information originate route-map default-condition
```

The following example shows how to configure BGP to accept routing updates from 192.1.1.1 only, besides filtering on the prefix length:

```
router bgp
distribute-list prefix max24 gateway allowlist in
!
ip prefix-list allowlist seq 5 permit 192.1.1.1/32
!
```

The following example shows how to direct the BGP process to filter incoming updates to the prefix using name1, and match the gateway (next hop) of the prefix being updated to the prefix list name2, on the Ethernet interface 0:

```
router bgp 103
distribute-list prefix name1 gateway name2 in ethernet 0.
```

Route Filtering Configuration Example Specifying a Group of Prefixes

The following example shows how to configure BGP to permit routes with a prefix length up to 24 in network 192/8:

```
ip prefix-list abc permit 192.0.0.0/8 1e 24
```

The following example shows how to configure BGP to deny routes with a prefix length greater than in 25 in 192/8:

```
ip prefix-list abc deny 192.0.0.0/8 ge 25
```

The following example shows how to configure BGP to permit routes with a prefix length greater than 8 and less than 24 in all address space:

```
ip prefix-list abc permit 0.0.0.0/0 ge 8 1e 24
```

The following example shows how to configure BGP to deny routes with a prefix length greater than 25 in all address space:

```
ip prefix-list abc deny 0.0.0.0/0 ge 25
```

The following example shows how to configure BGP to deny all routes in 10/8, because any route in the Class A network 10.0.0.0/8 is denied if its mask is less than or equal to 32 bits:

```
ip prefix-list abc deny 10.0.0.0/8 1e 32
```

The following example shows how to configure BGP to deny routes with a mask greater than 25 in 204.70.1/24:

```
ip prefix-list abc deny 204.70.1.0/24 ge 25
```

The following example shows how to configure BGP to permit all routes:

```
ip prefix-list abc permit 0.0.0.0/0 1e 32
```

23.320

Added or Deleted Prefix List Entries Examples

You can add or delete individual entries in a prefix list if a prefix list has the following initial configuration:

```
ip prefix-list abc deny 0.0.0.0/0 le 7
ip prefix-list abc deny 0.0.0.0/0 ge 25
ip prefix-list abc permit 35.0.0.0/8
ip prefix-list abc permit 204.70.0.0/15
```

The following example shows how to delete an entry from the prefix list so that 204.70.0.0 is not permitted, and add a new entry that permits 198.0.0.0/8:

```
no ip prefix-list abc permit 204.70.0.0/15
ip prefix-list abc permit 198.0.0.0/8
```

The new configuration is as follows:

```
ip prefix-list abc deny 0.0.0.0/0 le 7
ip prefix-list abc deny 0.0.0.0/0 ge 25
ip prefix-list abc permit 35.0.0.0/8
ip prefix-list abc permit 198.0.0.0/8
```

BGP Soft Reset Examples

The following examples show two ways to reset the connection for BGP peer 131.108.1.1.

Dynamic Inbound Soft Reset Example

The following examples shows the **clear ip bgp 131.108.1.1 soft in** EXEC command used to initiate a dynamic soft reconfiguration in the BGP peer 131.108.1.1. This command requires that the peer support the route refresh capability.

```
clear ip bgp 131.108.1.1 soft in
```

Inbound Soft Reset Using Stored Information Example

The following example shows how to enable inbound soft reconfiguration for the neighbor 131.108.1.1. All the updates received from this neighbor will be stored unmodified, regardless of the inbound policy. When inbound soft reconfiguration is performed later, the stored information will be used to generate a new set of inbound updates.

```
router bgp 100
 neighbor 131.108.1.1 remote-as 200
 neighbor 131.108.1.1 soft-reconfiguration inbound
```

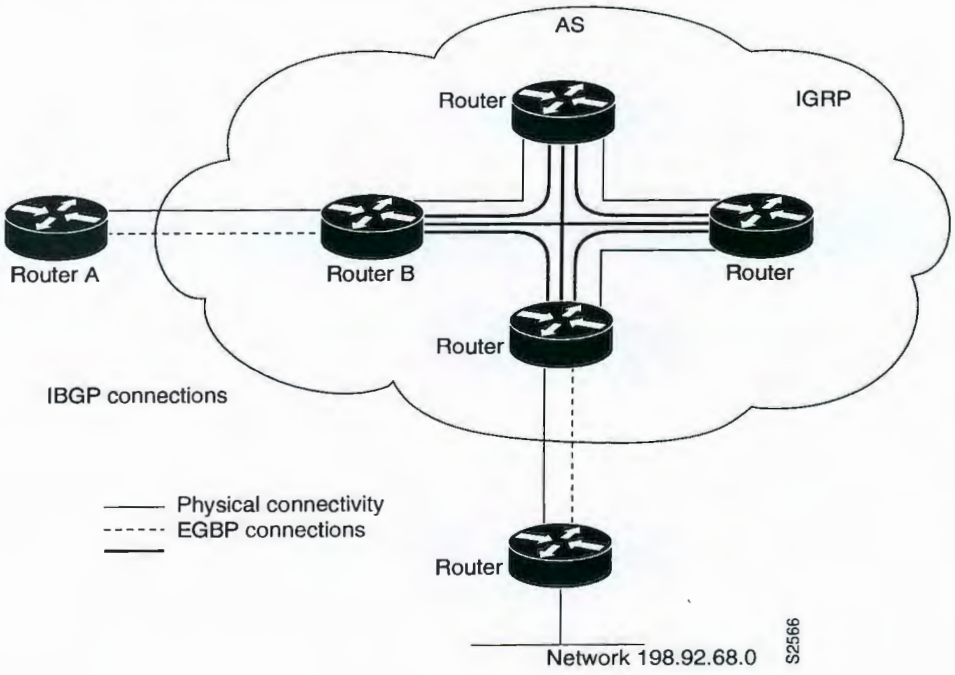
The following example clears the session with the neighbor 131.108.1.1.

```
clear ip bgp 131.108.1.1 soft in
```

BGP Synchronization Examples

The example shown in Figure 57 shows how to use the **no synchronization** router configuration command. In the figure, synchronization is on, and Router B does not advertise network 198.92.68.0 to Router A until an IGRP route for network 198.92.68.0 exists. If you specify the **no synchronization** router configuration command, Router B advertises network 198.92.68.0 as soon as possible. However, because routing information still must be sent to interior peers, you must configure a full iBGP mesh.

Figure 57 BGP Synchronization Configuration



BGP Path Filtering by Neighbor Examples

The following example shows BGP path filtering by neighbor. Only the routes that pass autonomous system path access list 2 will be sent to 193.1.12.10. Similarly, only routes passing access list 3 will be accepted from 193.1.12.10.

```
router bgp 200
 neighbor 193.1.12.10 remote-as 100
 neighbor 193.1.12.10 filter-list 1 out
 neighbor 193.1.12.10 filter-list 2 in
ip as-path access-list 1 permit _109_
ip as-path access-list 2 permit _200$
ip as-path access-list 2 permit ^100$
ip as-path access-list 3 deny _690$
ip as-path access-list 3 permit .*
```

23.818

BGP Aggregate Route Examples

The following examples show how you can use aggregate routes in BGP either by redistributing an aggregate route into BGP or by using the BGP Conditional Aggregate routing feature.

In the following example, the **redistribute static** router configuration command is used to redistribute aggregate route 193.0.0.0:

```
ip route 193.0.0.0 255.0.0.0 null 0
!
router bgp 100
 redistribute static
```

The following configuration shows how to create an aggregate entry in the BGP routing table when at least one specific route falls into the specified range. The aggregate route will be advertised as coming from your autonomous system and has the atomic aggregate attribute set to show that information might be missing. (By default, atomic aggregate is set unless you use the **as-set** keyword in the **aggregate-address** router configuration command.)

```
router bgp 100
 aggregate-address 193.0.0.0 255.0.0.0
```

The following example shows how to create an aggregate entry using the same rules as in the previous example, but the path advertised for this route will be an AS_SET consisting of all elements contained in all paths that are being summarized:

```
router bgp 100
 aggregate-address 193.0.0.0 255.0.0.0 as-set
```

The following example shows how to create the aggregate route for 193.0.0.0 and also suppress advertisements of more specific routes to all neighbors:

```
router bgp 100
 aggregate-address 193.0.0.0 255.0.0.0 summary-only
```

BGP Community with Route Maps Examples

This section contains three examples of the use of BGP communities with route maps, and two examples that also contain confederation configurations. For an example of how to configure a BGP confederation, see the section "BGP Confederation Examples" in this chapter.

The first example shows how the route map named set-community is applied to the outbound updates to the neighbor 171.69.232.50. The routes that pass access list 1 have the special community attribute value no-export. The remaining routes are advertised normally. This special community value automatically prevents the advertisement of those routes by the BGP speakers in autonomous system 200.

```
router bgp 100
 neighbor 171.69.232.50 remote-as 200
 neighbor 171.69.232.50 send-community
 neighbor 171.69.232.50 route-map set-community out
!
route-map set-community 10 permit
 match address 1
 set community no-export
!
route-map set-community 20 permit
 match address 2
```

The second example shows how the route map named set-community is applied to the outbound updates to neighbor 171.69.232.90. All the routes that originate from autonomous system 70 have the community values 200 200 added to their already existing values. All other routes are advertised as normal.

```
route-map bgp 200
 neighbor 171.69.232.90 remote-as 100
 neighbor 171.69.232.90 send-community
 neighbor 171.69.232.90 route-map set-community out
!
route-map set-community 10 permit
 match as-path 1
 set community 200 200 additive
!
route-map set-community 20 permit
!
ip as-path access-list 1 permit 70$
ip as-path access-list 2 permit .*
```

The third example shows how community-based matching is used to selectively set MED and local preference for routes from neighbor 171.69.232.55. All the routes that match community list 1 get the MED set to 8000, including any routes that have the communities 100 200 300 or 900 901. These routes could have other community values also.

All the routes that pass community list 2 get the local preference set to 500. This includes the routes that have community values 88 or 90. If they belong to any other community, they will not be matched by community list 2.

All the routes that match community list 3 get the local preference set to 50. Community list 3 will match all the routes because all the routes are members of the Internet community. Thus, all the remaining routes from neighbor 171.69.232.55 get a local preference 50.

```
router bgp 200
 neighbor 171.69.232.55 remote-as 100
 neighbor 171.69.232.55 route-map filter-on-community in
!
route-map filter-on-community 10 permit
 match community 1
 set metric 8000
!
route-map filter-on-community 20 permit
 match community 2 exact-match
 set local-preference 500
!
route-map filter-on-community 30 permit
 match community 3
 set local-preference 50
!
ip community-list 1 permit 100 200 300
ip community-list 1 permit 900 901
!
ip community-list 2 permit 88
ip community-list 2 permit 90
!
ip community-list 3 permit internet
```

The next two examples show how BGP community attributes are used with BGP confederation configurations to filter routes.

The next example shows how the route map named set-community is applied to the outbound updates to neighbor 171.69.232.50 and the local-as community attribute is used to filter the routes. The routes that pass access list 1 have the special community attribute value local-as. The remaining routes are advertised normally. This special community value automatically prevents the advertisement of those routes by the BGP speakers outside autonomous system 200.

```
router bgp 65000
 network 1.0.0.0 route-map set-community
 bgp confederation identifier 200
 bgp confederation peers 65001
 neighbor 171.69.232.50 remote-as 100
 neighbor 171.69.233.2 remote-as 65001
!
route-map set-community permit 10
 match ip address 1
 set community local-as
!
```

The following example shows how to use the local-as community attribute to filter the routes. Confederation 100 contains three autonomous systems: 100, 200, and 300. For network 1.0.0.0, the route map named set-local-as specifies that the advertised routes have the community attribute local-as. These routes are not advertised to any eBGP peer outside the local autonomous system. For network 2.0.0.0, the route map named set-no-export specifies that the routes advertised have the community attribute no-export.

A route between router 6500 and router 65001 does not cross the boundary between autonomous systems within the confederation. A route between subautonomous systems for which router 65000 is the controlling router does not cross the boundary between the confederation and an external autonomous system, and also does not cross the boundary between subautonomous systems within the local autonomous system. A route to from router 65000 to router 65001 would not be acceptable for network 1.0.0.0 because it crosses the boundary between subautonomous systems within the confederation.

```
router bgp 65001
 bgp confederation identifier 200
 bgp confederation peer 65000
 network 2.0.0.0 route-map  set-community
 neighbor 171.69.233.1 remote-as 65000
route-map set-community permit 10
 set community no-export
```

BGP Conditional Advertisement Configuration Examples

This section provides a configuration example of the BGP Conditional Advertisement feature. In the following example, the *ip-address* argument refers to the IP address of the neighbor, and the *map1-name* and *map2-name* arguments, refer to the names of the route maps:

neighbor {*ip-address*} **advertise-map** {*map1-name*} **non-exist-map** {*map2-name*}

no neighbor {*ip-address*} **advertise-map** {*map1-name*} **non-exist-map** {*map2-name*}

The route map associated with the non-exist-map specifies the prefix that the BGP speaker tracks. The route map associated with the advertise map specifies the prefix that is advertised when the prefix in the non-exist-map no longer exists. The prefix tracked by the BGP speaker must be present in the IP routing table for the conditional advertisement not to take place. In the following example, the router advertises 172.16.0.0/16 to its neighbor only if 192.168.7.0/24 is not present in the IP routing table.

To conditionally advertise a set of routes, use the following commands in router configuration mode:

```
router bgp 109
```

```
neighbor 10.89.2.33 remote-as 2051
neighbor 10.89.2.33 advertise-map map1-name non-exist-map map2-name
route-map map1-name permit 10
match ip address 1
route-map map2-name permit 10
match ip address 2
access-list 1 permit 172.16.0.0
access-list 2 permit 192.168.7.0
```

BGP Confederation Examples

The following is a sample configuration that shows several peers in a confederation. The confederation consists of three internal autonomous systems with autonomous system numbers 6001, 6002, and 6003. To the BGP speakers outside the confederation, the confederation looks like a normal autonomous system with autonomous system number 666 (specified via the **bgp confederation identifier** router configuration command).

In a BGP speaker in autonomous system 6001, the **bgp confederation peers** router configuration command marks the peers from autonomous systems 6002 and 6003 as special eBGP peers. Hence peers 171.69.232.55 and 171.69.232.56 will get the local preference, next hop, and MED unmodified in the updates. The router at 160.69.69.1 is a normal eBGP speaker and the updates received by it from this peer will be just like a normal eBGP update from a peer in autonomous system 666.

```
router bgp 6001
 bgp confederation identifier 666
 bgp confederation peers 6002 6003
 neighbor 171.69.232.55 remote-as 6002
 neighbor 171.69.232.56 remote-as 6003
 neighbor 160.69.69.1 remote-as 777
```

In a BGP speaker in autonomous system 6002, the peers from autonomous systems 6001 and 6003 are configured as special eBGP peers. 170.70.70.1 is a normal iBGP peer and 199.99.99.2 is a normal eBGP peer from autonomous system 700.

```
router bgp 6002
 bgp confederation identifier 666
 bgp confederation peers 6001 6003
 neighbor 170.70.70.1 remote-as 6002
 neighbor 171.69.232.57 remote-as 6001
 neighbor 171.69.232.56 remote-as 6003
 neighbor 199.99.99.2 remote-as 700
```

In a BGP speaker in autonomous system 6003, the peers from autonomous systems 6001 and 6002 are configured as special eBGP peers. 200.200.200.200 is a normal eBGP peer from autonomous system 701.

```
router bgp 6003
 bgp confederation identifier 666
 bgp confederation peers 6001 6002
 neighbor 171.69.232.57 remote-as 6001
 neighbor 171.69.232.55 remote-as 6002
 neighbor 200.200.200.200 remote-as 701
```

The following is a part of the configuration from the BGP speaker 200.200.200.205 from autonomous system 701 in the same example. Neighbor 171.69.232.56 is configured as a normal eBGP speaker from autonomous system 666. The internal division of the autonomous system into multiple autonomous systems is not known to the peers external to the confederation.

```
router bgp 701
 neighbor 171.69.232.56 remote-as 666
```

```
neighbor 200.200.200.205 remote-as 701
```

For examples of how the BGP **set-community** route-map configuration command can be used with a confederation configuration, see the last two examples in the section"BGP Community with Route Maps Examples" in this chapter.

BGP Peer Group Examples

This section contains an iBGP peer group example and an eBGP peer group example.

iBGP Peer Group Example

The following example shows how the peer group named internal configures the members of the peer group to be iBGP neighbors. By definition, this is an iBGP peer group because the **router bgp** global configuration command and the **neighbor remote-as** router configuration command indicate the same autonomous system (in this case, autonomous system 100). All the peer group members use loopback 0 as the update source and use set-med as the outbound route map. The example also shows that, except for the neighbor at address 171.69.232.55, all the neighbors have filter list 2 as the inbound filter list.

```
router bgp 100
 neighbor internal peer-group
 neighbor internal remote-as 100
 neighbor internal update-source loopback 0
 neighbor internal route-map set-med out
 neighbor internal filter-list 1 out
 neighbor internal filter-list 2 in
 neighbor 171.69.232.53 peer-group internal
 neighbor 171.69.232.54 peer-group internal
 neighbor 171.69.232.55 peer-group internal
 neighbor 171.69.232.55 filter-list 3 in
```

eBGP Peer Group Example

The following example shows how the peer group named external-peers is defined without the **neighbor remote-as** router configuration command, making it an eBGP peer group. Each member of the peer group is configured with its respective autonomous system number separately. Thus, the peer group consists of members from autonomous systems 200, 300, and 400. All the peer group members have set-metric route map as an outbound route map and filter list 99 as an outbound filter list. Except for neighbor 171.69.232.110, all have 101 as the inbound filter list.

```
router bgp 100
 neighbor external-peers peer-group
 neighbor external-peers route-map set-metric out
 neighbor external-peers filter-list 99 out
 neighbor external-peers filter-list 101 in
 neighbor 171.69.232.90 remote-as 200
 neighbor 171.69.232.90 peer-group external-peers
 neighbor 171.69.232.100 remote-as 300
 neighbor 171.69.232.100 peer-group external-peers
 neighbor 171.69.232.110 remote-as 400
 neighbor 171.69.232.110 peer-group external-peers
 neighbor 171.69.232.110 filter-list 400 in
```

TCP MD5 Authentication for BGP Examples

The following example specifies that the router and its BGP peer at 145.2.2.2 invoke MD5 authentication on the TCP connection between them:

```
router bgp 109
 neighbor 145.2.2.2 password v61ne0qkel33&
```

23.812

Configuring Policy-Based Routing

This chapter describes the tasks for configuring policy-based routing (PBR) on a router.

For complete conceptual information about this feature, see the section "Policy-Based Routing" in the chapter "Classification Overview" in this book.

For a complete description of the PBR commands in this chapter, refer to the *Cisco IOS Quality of Service Solutions 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 "Using Cisco IOS Software" chapter in this book.

Policy-Based Routing Configuration Task List

To configure PBR, perform the tasks described in the following sections. The task in the first section is required; the tasks in the remaining sections are optional.

- Enabling PBR (Required)
- Enabling Fast-Switched PBR (Optional)
- Enabling Local PBR (Optional)

See the end of this chapter for the section "Policy-Based Routing Configuration Examples."

Enabling PBR

To enable PBR, you must create a route map that specifies the match criteria and the resulting action if all of the match clauses are met. Then, you must enable PBR for that route map on a particular interface. All packets arriving on the specified interface matching the match clauses will be subject to PBR.

To enable PBR on an interface, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# route-map map-tag [permit | deny] [sequence-number]`	Defines a route map to control where packets are output. This command puts the router into route-map configuration mode.

Step 2	`Router(config-route-map)# match length min max`
	
	`Router(config-route-map)# match ip address {access-list-number | name} [...access-list-number | name]`
		Specifies the match criteria. You can specify one or both of the following:
		• Matches the Level 3 length of the packet.
		• Matches the source and destination IP address that is permitted by one or more standard or extended access lists.
		If you do not specify a **match** command, the route map applies to all packets.

Step 3	`Router(config-route-map)# set ip precedence [number | name]`
	
	`Router(config-route-map)# set ip next-hop ip-address [... ip-address]`
	
	`Router(config-route-map)# set interface interface-type interface-number [... type number]`
	`Router(config-route-map)# set ip default next-hop ip-address [... ip-address]`
	
	`Router(config-route-map)# set default interface interface-type interface-number [... type ...number]`
		Specifies the action or actions to take on the packets that match the criteria. You can specify any or all of the following:
		• Sets precedence value in the IP header. You can specify either the precedence number or name.
		• Sets next hop to which to route the packet (the next hop must be adjacent).
		• Sets output interface for the packet.
		• Sets next hop to which to route the packet, if there is no explicit route for this destination.
		• Sets output interface for the packet, if there is no explicit route for this destination.

Step 4	`Router(config-route-map)# interface interface-type interface-number`	Specifies the interface. This command puts the router into interface configuration mode.
Step 5	`Router(config-if)# ip policy route-map map-tag`	Identifies the route map to use for PBR. One interface can only have one route map tag, but you can have multiple route map entries with different sequence numbers. These entries are evaluated in sequence number order until the first match. If there is no match, packets will be routed as usual.

The **set** commands can be used in conjunction with each other. They are evaluated in the order shown Step 3 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.

Note Enabling PBR disables fast switching of all packets arriving on this interface.

If you want PBR to be fast-switched, see the section "Enabling Fast-Switched PBR," which follows.

Enabling Fast-Switched PBR

IP PBR can now be fast-switched. Prior to Cisco IOS Release 12.0, PBR could only be process-switched, which meant that on most platforms the switching rate was approximately 1000 to 10,000 packets per second. This speed was not fast enough for many applications. Users that need PBR to occur at faster speeds can now implement PBR without slowing down the router.

Fast-switched PBR supports all of the **match** commands and most of the **set** commands, with the following restrictions:

- The **set ip default next-hop** and **set default interface** commands are 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.

PBR must be configured before you configure fast-switched PBR. Fast switching of PBR is disabled by default. To enable fast-switched PBR, use the following command in interface configuration mode:

Command	Purpose
`Router(config-if)# ip route-cache policy`	Enables fast switching of PBR.

To display the cache entries in the policy route cache, use the **show ip cache policy** command. To display which route map is associated with which interface, use the **show ip policy** command.

Enabling Local PBR

Packets that are generated by the router are not normally policy-routed. To enable local PBR for such packets, indicate which route map the router should use by using the following command in global configuration mode:

Command	Purpose
`Router(config)# ip local policy route-map` *map-tag*	Identifies the route map to use for local PBR.

All packets originating on the router will then be subject to local PBR.

Use the **show ip local policy** command to display the route map used for local PBR, if one exists.

Policy-Based Routing Configuration Examples

The following sections provide PBR configuration examples:

- Equal Access Example
- Differing Next Hops Example

For information on how to configure policy-based routing, see the section "Policy-Based Routing Configuration Task List" in this chapter.

Equal Access 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
```

Differing Next Hops Example

The following example illustrates how to route traffic from different sources to different places (next hops), and how to set the Precedence bit in the IP header. Packets arriving from source 1.1.1.1 are sent to the next hop at 3.3.3.3 with the Precedence bit set to priority; packets arriving from source 2.2.2.2 are sent to the next hop at 3.3.3.5 with the Precedence bit set to critical.

```
access-list 1 permit ip 1.1.1.1
access-list 2 permit ip 2.2.2.2
!
interface ethernet 1
 ip policy route-map Texas
!
route-map Texas permit 10
 match ip address 1
 set ip precedence priority
 set ip next-hop 3.3.3.3
!
route-map Texas permit 20
 match ip address 2
 set ip precedence critical
 set ip next-hop 3.3.3.5
```

Data Sheet

Cisco 2600, 3600 and 3700 Voice Gateway Router
Router Interoperability with Cisco CallManager

Cisco 2600, 3600 and 3700 multiservice platforms can be deployed as Voice Gateway Routers as part of the Cisco AVVID (Architecture for Voice, Video and Integrated Data)-enabled Cisco CallManager IP telephony solution. New and existing deployments can benefit by using 2600/3600/3700 multiservice platforms as Voice Gateway Routers with Cisco CallManager. Cisco 2600, 3600 and 3700 Voice Gateway Routers communicate directly with Cisco CallManager, allowing for the deployment of IP telephony solutions that are ideal for large enterprises and service providers that offer network managed services. The Cisco 2600/3600/3700 Voice Gateway Router capability leverages an award-winning modular platform that is designed to provide a highly flexible, scalable, multiservice solution for small and medium-sized branches and regional offices. The Cisco 2600/3600/3700 Voice Gateway Router supports the widest range of packet telephony- based voice interfaces and signaling protocols within the industry, providing connectivity support for over 90 percent of the world's private branch exchanges (PBXs) and public switched telephone network (PSTN) connection points. Signaling support includes T1-PRI, E1-PRI, T1-CAS, E1- R2, T1/E1 QSIG, T1 FGD, BRI, FXO, E&M and FXS. The Cisco 2600, 3600 and 3700 Voice Gateway Routers can be configured to support from two to 300 voice channels. As enterprises seek to deploy an expanding list of IP telephony applications and services, Cisco 2600, 3600 and 3700 Voice Gateway Routers, interoperating with Cisco CallManager, provide a solution that will grow with the changing needs of enterprises.

Interoperability Using H.323 or MGCP

The Cisco 2600/3600/3700 Voice Gateway Routers can communicate with the Cisco CallManager using H.323 or Media Gateway Control Protocol (MGCP):

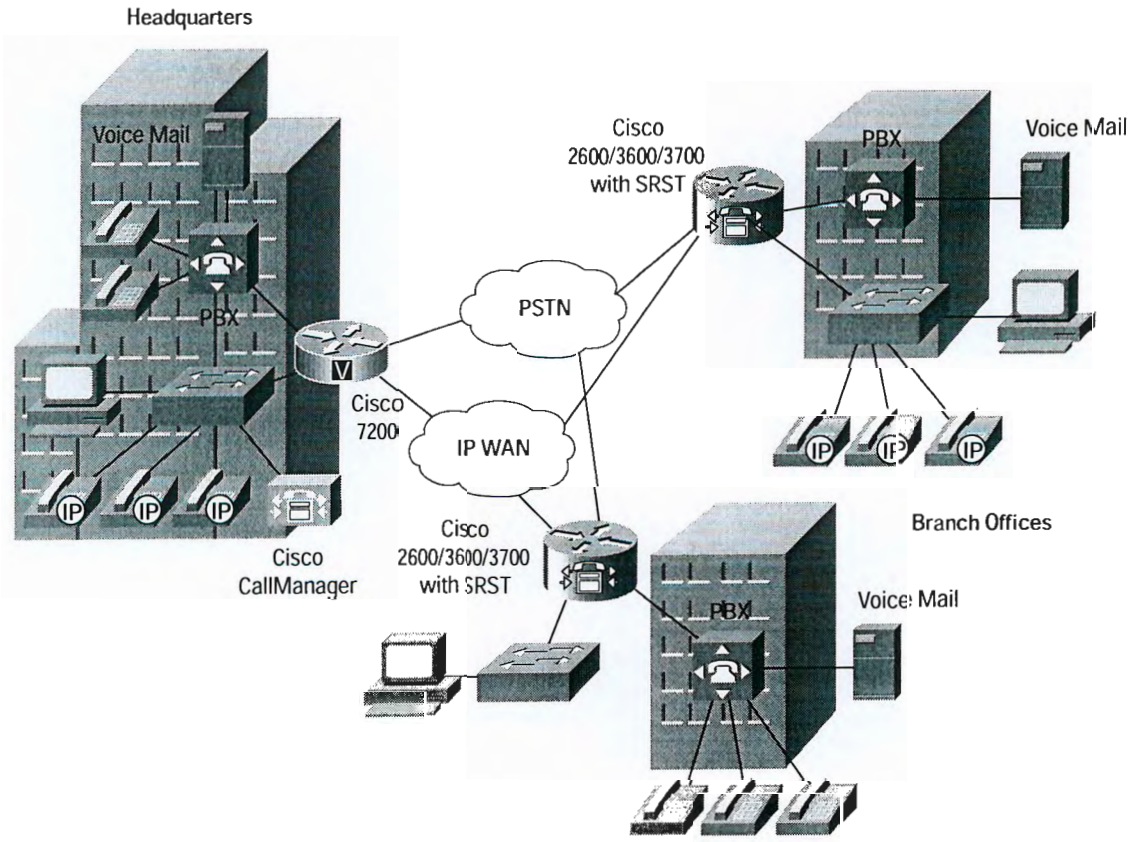
- In H.323 mode, the Cisco 2600/3600/3700 Voice Gateway Router communicates with Cisco CallManager as an intelligent gateway device.
- In MGCP mode, the Cisco 2600/3600/3700 Voice Gateway Router operates as a stateless client, giving Cisco CallManager full control.

As MGCP Voice Gateway Routers, Cisco 2600/3600/3700 multiservice platforms provide enhanced network management and failover capabilities. In MGCP mode, dial plans are configured centrally in Cisco CallManager, instead of in each gateway. And all Cisco 2600/3600/3700 MGCP Voice Gateway Routers in a Cisco AVVID-enabled IP telephony network can be automatically configured by downloading XML files from Cisco CallManager. Also, Cisco 2600/3600/3700 MGCP gateways provide multiple levels of failover capabilities, including Survivable/Standby Remote Site Telephony support to prevent call-processing interruptions or dropped calls in the event of a Cisco CallManager or WAN failure.

IP Telephony Phased Migration

The Cisco 2600/3600/3700 Voice Gateway Router enables users to immediately deploy an end-to-end IP telephony network architecture or gradually shift voice traffic from traditional circuit-switched networks to a single infrastructure carrying data, voice, and video over packet networks. Initially, customers can use the Cisco 2600/3600/3700 Voice Gateway Routers to interconnect legacy PBXs over the packet infrastructure and still maintain PSTN (off-net) connectivity via their circuit-switched PBXs. Later, customers can migrate PSTN (off-net) connectivity to the Voice Gateway Routers and start to incorporate IP phones at larger sites (Figure 1). After all sites are running IP telephony, users can begin deploying IP-based applications such as IP unified messaging, personal assistants, and extension mobility. The Cisco 2600/3600/3700 Voice Gateway Router is an ideal solution for circuit-switched PBX and PSTN access within a Cisco CallManager IP telephony architecture.

Figure 1
IP Telephony Phased Migration—Migrate Circuit-Switched PSTN and PBX Connectivity to Voice Gateway Routers



As companies seek to deploy IP telephony solutions across the entire enterprise—converging voice, video, and data across potentially thousands of sites—they require a feature-rich IP telephony solution that offers simple administration, virtually unlimited scalability and high availability. The Cisco 2600/3600/3700 MGCP Voice Gateway Routers work in concert with the Cisco CallManager, deployed in either a distributed or centralized call-processing model, to provide the IP telephony solutions that enterprises require.

13.805

Centralized Call-Processing

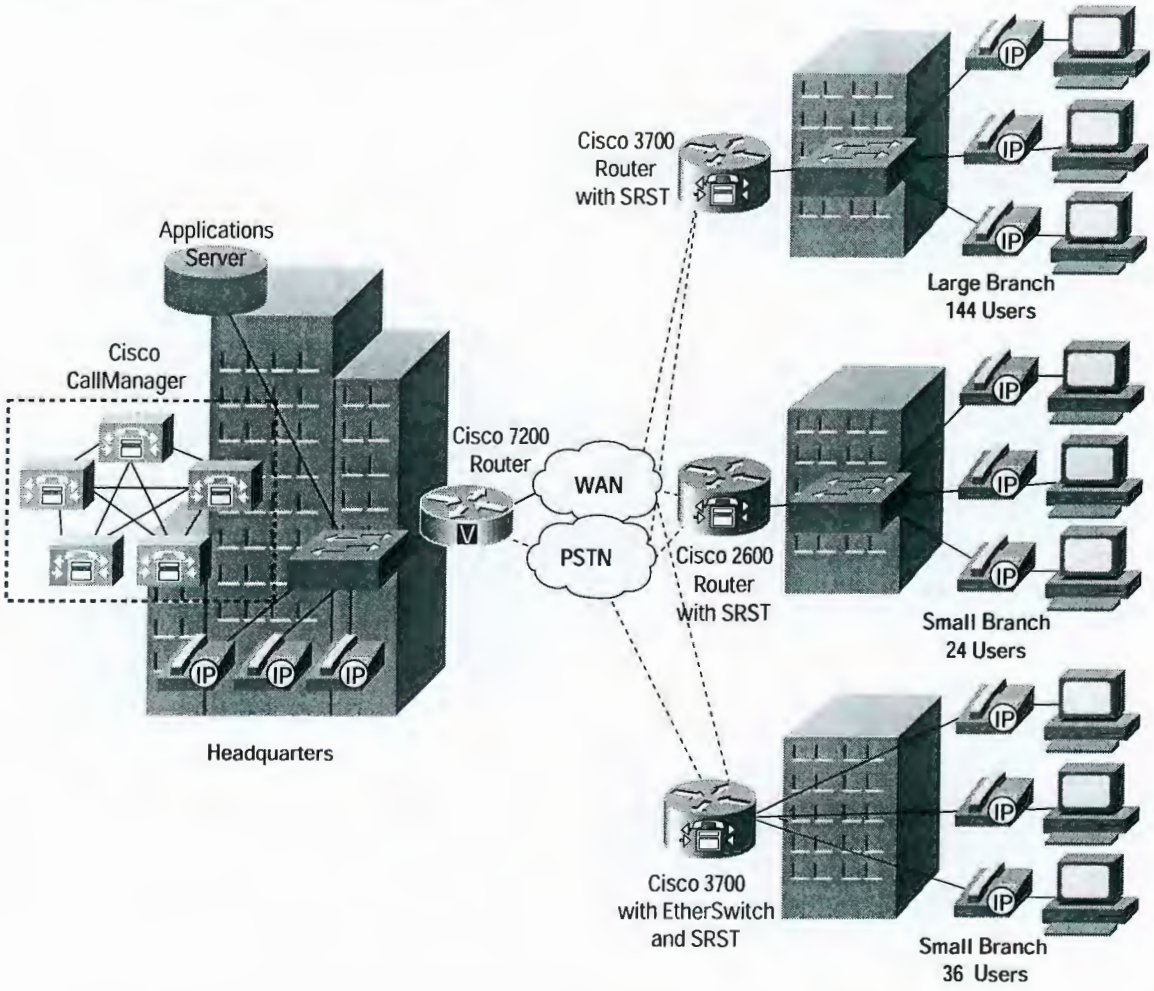
Demand for technology to support increased employee productivity and lower costs is at an all-time high. At the same time, many organizations are struggling to deploy new applications and services because of flat budgets. The centralized call-processing model can provide technology to users who require it, while simultaneously providing ease of centralized management and maintenance of applications to network administrators. Instead of deploying and managing key systems or PBXs in small offices, applications are centrally located at a corporate headquarters or data center, and accessed via the IP LAN and WAN. This deployment model allows branch office users to access the full enterprise suite of communications and productivity applications for the first time, while lowering total cost of ownership (TCO). There is no need to "touch" each branch office each time a software upgrade or new application is deployed, which accelerates the speed in which organizations can adopt and deploy new technology solutions. In the Internet economy, the ability to quickly roll out new applications to remote users can provide a sustainable competitive advantage versus companies that must visit each of their branch sites to take advantage of new applications. An architecture in which a Cisco CallManager and other Cisco AVVID applications are located at the central site has the following benefits:

- Centralized configuration and management
- Access at every site to all Cisco CallManager features, next-generation contact centers, unified messaging services, personal productivity tools, mobility solutions, and soft phones all the time
- IT staff is not required at each remote site
- Ability to rapidly deploy applications to remote users
- Easy upgrades and maintenance
- Lower TCO

Survivable/Standby Remote Site Telephony (SRS Telephony)

As enterprises extend their IP telephony deployments from central sites to remote offices, an important consideration is the ability to cost-effectively provide failover capability at remote branch offices. However, the size and number of these small-office sites preclude most enterprises from deploying dedicated call-processing servers, unified messaging servers, or multiple WAN links to each site to achieve the required high availability. The Cisco CallManager IP telephony solution with SRS Telephony allows companies to extend high-availability IP telephony to their remote branch offices with a cost-effective solution that is easy to deploy, administer, and maintain.The SRS Telephony capability is embedded in the Cisco IOS™ Software that runs on the Cisco 2600/3600/3700 Voice Gateway Router. SRS Telephony software automatically detects a connectivity failure between Cisco CallManager and IP phones at the branch office. Using the Cisco Simple Network Automated Provisioning (SNAP) capability, SRS Telephony initiates a process to intelligently auto-configure the Cisco 2600/3600/3700 Voice Gateway Router to provide call-processing backup redundancy for the IP phones in the affected office. The router provides essential call-processing services for the duration of the failure, ensuring that critical phone capabilities are operational. Upon restoration of the connectivity to the CallManager, the system automatically shifts call-processing functions back to the primary Cisco CallManager cluster. Configuration for this capability is done only once in the Cisco CallManager at the central site.

Figure 2
Centralized Cisco CallManager Deployment with SRS Telephony



Key 2600/3600/3700 MGCP Voice Gateway Router Features and Benefits

Simple Administration

- Provides centralized administration and management
- Enables administration of large dial plans
- Provides a single point of configuration for a Cisco AVVID-enabled IP telephony network

Availability

- Provides Cisco CallManager redundancy
- Provides call preservation for gateway calls when the host Cisco CallManager fails
- Provides MGCP gateway fallback to H.323 control for basic call-handling when the WAN fails

Scalability

- Meets enterprise office requirements of small offices to large corporations
- Scales up to 30,000 users per cluster with Cisco CallManager clustering.

Investment Protection

- Provides a modular platform design with a growing list of more than 90 interface combinations
- Allows users to increase voice capacity while leveraging their existing investment in Cisco 2600, 3600 and 3700 multiservice platforms

Voice Gateway Router with Cisco CallManager Minimum System Requirements

Table 1 Cisco 2600, 3600, 3700, Access Gateway Module and VG200

Signaling	MGCP	H.323
Analog (FXS, FXO)	Cisco IOS: 12.2(4)T Cisco CallManager: 3.0(5a)	Cisco IOS: 12.2(1)M Cisco CallManager: 3.0(5a)
BRI	Cisco IOS: 12.2(15)ZJ Cisco CallManager: 3.3(2)FP1 (This is a controlled release version of Cisco CallManager and is the only release that currently provides this feature.)	Cisco IOS: 12.2(1)M Cisco CallManager: 3.0(5a)
T1 CAS, T1/E1 PRI	Cisco IOS: 12.2(11)T Cisco CallManager: 3.1(1)	Cisco IOS: 12.1(2)T Cisco CallManager: 3.0(5a)
T1/E1 QSIG	Cisco IOS: 12.2(11)T Cisco CallManager: 3.3(2)	Cisco IOS: 12.1(2)T Cisco CallManager: 3.0(5a)

1. The Cisco 2691, 3725 and 3745 is supported with Cisco IOS 12.2(8)T1 or later and Cisco CallManager 3.2(2c)spA or later.
2. The Access Gateway Module is supported with Cisco IOS 12.2(13)T or later and Cisco CallManager 3.2(2c)spB or later.
3. MGCP is not supported for BRI on the VG200 or Access Gateway Module.
4. The actual DRAM and Flash requirements may vary depending on the particular platform and version of Cisco IOS software used. Please refer to the release notes for the version of Cisco IOS software being used for the exact Flash and DRAM requirements.
5. Network module support and required software may vary. Please refer to the Cisco IOS Release Notes and Cisco CallManager Release Notes for definition of features supported.
6. The IP Communications Voice/Fax Network Module (NM-HD) requires Cisco IOS 12.2(15)ZJ. Cisco CallManager 3.3(3) is required for MGCP support.

Voice Gateway Router with Cisco CallManager Feature Summary

Table 2 Voice Gateway Router with Cisco CallManager Feature Summary

MGCP	H.323	Feature	Benefits
X	X	Analog FXS (Foreign Exchange Station) interfaces loop-start and ground-start signaling	Enable direct connection to phones, fax machines, and key systems
	X	Analog E&M (wink, immediate, delay) interfaces	Enable direct connection to a PBX
X	X	Analog FXO (Foreign Exchange Station) interfaces loop-start and ground-start signaling	Enables connecting to a PBX or key system and provides off-premise connections to/from the PSTN/PTT
	X	Analog (Direct Inward Dial) DID	Enable connection to PSTN
	X	Analog CAMA	Enables PSTN connection for 911 Support
	X	BRI Q.931 network side (NET3)	Enables connection to a PBX or key system
X	X	BRI Q.931 user side (NET3)	Enables connection to PSTN
	X	BRI Q.SIG	Enables connection to a PBX or key system
X	X	T1-CAS E&M (wink start and immediate start) interfaces	Enables connection to a PBX or key system
	X	T1-CAS E&M (delay dial) interfaces	Enable connection to a PBX or key system
	X	T1-CAS FGD	Use to connect to a PBX or PSTN
	X	T1-CAS FXO (ground start and loop start) interfaces	Use to connect to PBX or key system and to provide off-premise connections
	X	T1-CAS FXS (ground start and loop start) interfaces	Use to connect to PBX or key system
	X	E1 CAS	Enable connection to a PBX or PSTN
	X	E1 MeICAS	Enable connection to a PBX or PSTN
	X	E1 R2 (more than 30 country variants)	Enable connection to a PBX or PSTN
X	X	T1/E1 ISDN PRI Q.931 interfaces	Use to connect to PBX or key system and to provide off-premise connections to/from the PSTN/PTT
X	X	T1 and E1 Q.SIG	Use to connect to PBX
X	X	Out-of-Band DTMF	Carry DTMF tones and information out of band for clearer transmission and detection.
X	X	Supplementary services	Enable hold, transfer, forward, and conference capabilities from an IP Phone
X		Single point of configuration for a Cisco AVVID-enabled IP telephony network	Centralizes and automates the configuration process for MGCP Voice Gateway Routers by making them configurable on the Cisco CallManager. Configuration information is automatically downloaded at startup and after any configuration change

Table 2 Voice Gateway Router with Cisco CallManager Feature Summary

MGCP	H.323	Feature	Benefits
X		XML configuration files for single-point configuration	MGCP Voice Gateway Router configuration information is stored in XML file format on a Cisco CallManager server and can be easily manipulated with any standard Web browser
X	X	Cisco CallManager failover redundancy	When a MGCP Voice Gateway Router loses contact with the primary CallManager the gateway reregisters with the next available Cisco CallManager of the three on its list
X		MGCP gateway fallback	When the WAN connection to a main site MGCP CallManager is lost, MGCP gateway fallback provides basic call-handling support for PSTN telephony interfaces on a branch office gateway for the duration of the WAN outage
X	X	Multicast music on hold (MOH)	Enables the Voice Gateway Router to deliver music streams from an MOH server to users on on-net and off-net calls
X	X	Tone on hold	Tone indicates when a user is placed on hold
X	X	Caller ID support	Enables the Voice Gateway Router to send the ANI of a caller for display: In MGCP mode, to/from IP phones, FXS and T1/E1 PRI (Caller ID currently not supported on FXO and T1-CAS) In H.323 mode, between IP phones, FXS, BRI and T1/E1 PRI; and from FXO to IP Phones, FXS, BRI and T1/E1 PRI
X	X	Platform voice scalability	Scale from two to 300 voice channels in a single multiservice router solution
X	X	Modular design	Single box supports data and telephony services
X	X	Standards-based PCM encoding	ITU-T G.711 PCM encoding provides 64-kbps analog-to-digital conversion using u-law or A-law.

Table 3 Voice Gateway Router Feature Summary

MGCP	H.323	Feature	Benefits
X	X	Standards-based compression algorithm support	Users can choose to either transmit voice across their networks as uncompressed PCM or compressed from 5.3 kbps to 32 kbps using standards-based compression algorithms (G.729, G.729a/b, G.723.1, G.726, and G.728).
X	X	Fax support	Transmit Group III fax over any voice channel without sacrificing voice-processing resources regardless of compression type being used.
X	X	Voice over IP (VoIP)	Transmit data, voice, and video across a single WAN connection (frame relay, ATM, ISDN, HDLC, or multilink point-to-point protocol [MLPPP]).
	X	Private Line Automatic Ringdown (PLAR)	Provides a dedicated connection to another phone or an auto attendant
	X	Connection trunk	Create permanent connection across the network, often to carry proprietary PBX signaling
	X	Off-premise extension (OPX)	Extend the capability of legacy PBX to off-premise phones. (This applies to toll-bypass applications only)
X	X	Voice Activity Detection (VAD)	Conserve bandwidth during a call when there is no active voice traffic to send
	X	Busy Out	Busy out desired trunk line to PBX when direct WAN or LAN connection to router is down
X	X	Comfort noise generation	While using VAD, the DSP at destination end emulates background noise from on the source side preventing the perception that a call is disconnected
	X	H.323 version 1, 2, 3, 4 support	Use industry-standard signaling protocols for call setup between gateways, gatekeepers, and H.323 endpoints
X	X	Authentication, Authorization, and Accounting (AAA)	Support debit card and credit card (prepaid and postpaid calling card) applications
	X	Interactive Voice Response (IVR) support	Enables automated attendant support, voice-mail support or call routing based on service desired
	X	Automated Attendant (AA)	Uses IVR to provide automated call answering and forwarding services

Telephony Interface Signaling Support

Table 4 Voice Performance on the Cisco VG200 and Cisco 2600, 3600 and 3700 Series Gateways for 12.2.8T

	2610	2610-XM [5]	VG200	2620	2620-XM[5]	2650 [5]	2650-XM [5]	3620	3640	2691 [3]	3725 [4]	3660	3745 [4]
VoIP Performance: Maximum													
Standalone Voice Gateway Router	48[1]	60[1]	60[2]	60[1]	70[1]	90[2]	90[2]	60[2]	96[1]	90[2]	120[2]	300[1]	240[2]
WAN Edge Gateway	24[1]	30[1]	N/A	30[1]	35[1]	60[1]	60[1]	30[1]	50[1]	90[2]	120[2]	200[1]	240[2]
WAN Edge Gateway with cRTP	12[1]	22[1]	N/A	22[1]	25[1]	42[1]	42[1]	24[1]	30[1]	90[2]	120[2]	160[1]	240[2]
VoIP Performance: Maximum Calls Per Second[1]													
	0.5	0.5	1	1	1	2	2	1	2	4	15	4	20
Maximum Physical DS0 Conn													
FXS	12	12	4	12	12	12	12	12	36	12	24	72	48
FXO	8	8	4	8	8	8	8	8	24	8	16	48	32
E&M	4	4	4	4	4	4	4	4	12	4	8	24	16
Analog DID	4	4	4	4	4	4	4	4	12	4	8	24	16
BRI	4	4	4	4	4	4	4	4	12	4	8	24	16
T1/E1 Ports	3	3	2	3	3	3	3	2	6	2/3	4/6	12	8/10
T1 Channels	72	72	48	72	72	72	72	48	144	48/72	96/120	288	192/240
E1 Channels	90	90	60	90	90	90	90	60	180	60/90	120/180	360	240/300

All results represent G.729 switched calls with VAD turned off.Standalone Voice Gateway Router: FE egress, no QoS features, Voice traffic only WAN Edge Gateway: T1/E1 Serial egress, QoS features (LLQ, LFI, TS), Voice (~50% of bandwidth) + Data traffic (~25% of bandwidth)

WAN Edge Gateway with cRTP: T1/E1 Serial egress, QoS features (LLQ, LFI, TS), cRTP, Voice (~50% of bandwidth) + Data traffic (~25% of bandwidth)

Notes:

1. 5% platform CPU utilization reached for this number of voice channels.
2. Physical DS0 connectivity limit reached for this configuration.
3. In 12.2.8T the 2691 supports a maximum 2 T1/E1s DS0 connectivity. In a later release, when the AIM-VOICE-30 is supported, the 2691 can support a maximum of 3 T1/E1 ports.
4. In 12.2.8T the 3725 and 3745 support a maximum 4 and 8 T1/E1s DS0 connectivity, respectively. In a later release, when the AIM-VOICE-30 is supported, the 3725 and 3745 will physically support a maximum of 6 and 10 T1/E1 ports, respectively. The capacity figures at that time may be revised to be higher.
5. 128M of memory equipped

For more information on Cisco 2600/3600/3700 multiservice platforms and Cisco IP telephony, visit: Digital T1/E1 Packet Voice Trunk Network Module Data Sheet: http://www.cisco.com/warp/public/cc/pd/rt/2600/prodlit/st1e1_ds.htm

- Low Density Voice/Fax Network Modules for the Cisco 2600, 3600 and 3700 Data Sheet: http://www.cisco.com/warp/public/cc/pd/rt/3600/prodlit/c36p_ds.htm
- Cisco SRS Telephony: http://www.cisco.com/warp/public/cc/pd/unco/srstl/index.shtml
- Cisco CallManager Version 3.1: http://www.cisco.com/warp/public/cc/pd/nemnsw/callmn/prodlit/callm_ds.htm
- Cisco AVVID for the Enterprise: http://www.cisco.com/warp/public/779/largeent/avvid/cisco_avvid.html

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

202867.J/ETMG_05/

ANEXO (19K)

Installing AC Power Supplies in Cisco 3725 Routers

Product Numbers: PWR-3725-AC=

This document describes how to replace the AC power supplies in a Cisco 3725 router.

This document is intended for the power supply installer, who should be familiar with electronic circuitry and wiring practices and have experience as an electronic or electromechanical technician. Use this document in conjunction with the *Cisco 3700 Series Hardware Installation Guide* and the *Regulatory Compliance and Safety Information* document for your router.

If you have questions or need help, refer to the "Obtaining Technical Assistance" section on page 19.

This document contains the following sections:

Warning **Only trained and qualified personnel should be allowed to install or replace this equipment. To see translations of the warnings that appear in this publication, refer to the *Regulatory Compliance and Safety Information* document that accompanied this device.**

Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Warning **Before working on a chassis or working near power supplies, unplug the power cord on AC units; disconnect the power at the circuit breaker on DC units. 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 **Before working on a system that has an on/off switch, turn OFF the power and unplug the power cord. 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 **Ultimate disposal of this product should be handled according to all national laws and regulations. To see translations of the warnings that appear in this publication, refer to the *Regulatory Compliance and Safety Information* document that accompanied this device.**

Caution To avoid damaging electrostatic discharge (ESD)-sensitive components, ensure that you have discharged all static electricity from your body before opening the chassis. Before performing procedures described in this document, review the next section, "Safety Recommendations."

Safety Recommendations

Follow these guidelines to ensure general safety:

- Keep the chassis area clear and dust-free during and after installation.
- Place the removed chassis cover in a safe place.
- Keep tools away from walk areas where you or others could fall over them.
- Do not wear loose clothing that may get caught in the chassis. Fasten your tie or scarf and roll up your sleeves.
- Wear safety glasses when working under conditions that may be hazardous to your eyes.
- Do not perform any action that creates a potential hazard to people or makes the equipment unsafe.

Warning **The ISDN connection is regarded as a source of voltage that should be inaccessible to user contact. Do not attempt to tamper with or open any public telephone operator (PTO)-provided equipment or connection hardware. Any hardwired connection (other than by a nonremovable, connect-one-time-only plug) must be made only by PTO staff or suitably trained engineers. 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 **The Ethernet 10BaseT, Token Ring, serial, console, and auxiliary ports contain safety extra-low voltage (SELV) circuits. BRI circuits are treated like telephone-network voltage (TNV) circuits. Avoid connecting SELV circuits to TNV circuits. To see translations of the warnings that appear in this publication, refer to the *Regulatory Compliance and Safety Information* document that accompanied this device.**

Safety with Electricity

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. To see translations of the warnings that appear in this publication, refer to the *Regulatory Compliance and Safety Information* document that accompanied this device.**

Follow these guidelines when working on equipment powered by electricity:

- Locate the room's emergency power-off switch. Then, if an electrical accident occurs, you can quickly shut the power off.
- Before working on the system, turn off the power and unplug the power cord.
- Disconnect all power before doing the following:
  - Working on or near power supplies
  - Installing or removing a router chassis or network processor module
  - Performing most hardware upgrades
- Do not work alone if potentially hazardous conditions exist.
- Look carefully for possible hazards in your work area, such as moist floors, ungrounded power extension cables, and missing safety grounds.
- Never assume that power is disconnected from a circuit. Always check.
- If an electrical accident occurs, proceed as follows:
  - Use caution, and do not become a victim yourself.
  - Turn off power to the system.
  - If possible, send another person to get medical aid. Otherwise, determine the condition of the victim and then call for help.
  - Determine if the person needs rescue breathing or external cardiac compressions; then take appropriate action.

Preventing Electrostatic Discharge Damage

Electrostatic discharge (ESD) can damage equipment and impair electrical circuitry. It occurs when electronic printed circuit cards are improperly handled and can result in complete or intermittent failures. Always follow ESD prevention procedures when removing and replacing cards. Ensure that the router chassis is electrically connected to earth ground. Wear an ESD-preventive wrist strap, ensuring that it makes good skin contact. Connect the clip to an unpainted surface of the chassis frame to safely channel unwanted ESD voltages to ground. To properly guard against ESD damage and shocks, the wrist strap and cord must operate effectively. If no wrist strap is available, ground yourself by touching the metal part of the chassis.

Caution For safety, periodically check the resistance value of the antistatic strap, which should be between 1 and 10 megohms (Mohms).

Safety Regulations

Warning Means *danger*. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. To see translations of the warnings that appear in this publication, refer to the *Regulatory Compliance and Safety Information* document that accompanied this device.

Waarschuwing Dit waarschuwingssymbool betekent gevaar. U verkeert in een situatie die lichamelijk letsel kan veroorzaken. Voordat u aan enige apparatuur gaat werken, dient u zich bewust te zijn van de bij elektrische schakelingen betrokken risico's en dient u op de hoogte te zijn van standaard maatregelen om ongelukken te voorkomen. Voor vertalingen van de waarschuwingen die in deze publicatie verschijnen, kunt u het document *Regulatory Compliance and Safety Information* (Informatie over naleving van veiligheids- en andere voorschriften) raadplegen dat bij dit toestel is ingesloten.

Varoitus Tämä varoitusmerkki merkitsee vaaraa. Olet tilanteessa, joka voi johtaa ruumiinvammaan. Ennen kuin työskentelet minkään laitteiston parissa, ota selvää sähkökytkentöihin liittyvistä vaaroista ja tavanomaisista onnettomuuksien ehkäisykeinoista. Tässä julkaisussa esiintyvien varoitusten käännökset löydät laitteen mukana olevasta *Regulatory Compliance and Safety Information* -kirjasesta (määräysten noudattaminen ja tietoa turvallisuudesta).

Attention Ce symbole d'avertissement indique un danger. Vous vous trouvez dans une situation pouvant causer des blessures ou des dommages corporels. Avant de travailler sur un équipement, soyez conscient des dangers posés par les circuits électriques et familiarisez-vous avec les procédures couramment utilisées pour éviter les accidents. Pour prendre connaissance des traductions d'avertissements figurant dans cette publication, consultez le document *Regulatory Compliance and Safety Information* (Conformité aux règlements et consignes de sécurité) qui accompagne cet appareil.

Warnung Dieses Warnsymbol bedeutet Gefahr. Sie befinden sich in einer Situation, die zu einer Körperverletzung führen könnte. Bevor Sie mit der Arbeit an irgendeinem Gerät beginnen, seien Sie sich der mit elektrischen Stromkreisen verbundenen Gefahren und der Standardpraktiken zur Vermeidung von Unfällen bewußt. Übersetzungen der in dieser Veröffentlichung enthaltenen Warnhinweise finden Sie im Dokument *Regulatory Compliance and Safety Information* (Informationen zu behördlichen Vorschriften und Sicherheit), das zusammen mit diesem Gerät geliefert wurde.

Avvertenza Questo simbolo di avvertenza indica un pericolo. La situazione potrebbe causare infortuni alle persone. Prima di lavorare su qualsiasi apparecchiatura, occorre conoscere i pericoli relativi ai circuiti elettrici ed essere al corrente delle pratiche standard per la prevenzione di incidenti. La traduzione delle avvertenze riportate in questa pubblicazione si trova nel documento *Regulatory Compliance and Safety Information* (Conformità alle norme e informazioni sulla sicurezza) che accompagna questo dispositivo.

Advarsel **Dette varselsymbolet betyr fare. Du befinner deg i en situasjon som kan føre til personskade. Før du utfører arbeid på utstyr, må du vare oppmerksom på de faremomentene som elektriske kretser innebærer, samt gjøre deg kjent med vanlig praksis når det gjelder å unngå ulykker. Hvis du vil se oversettelser av de advarslene som finnes i denne publikasjonen, kan du se i dokumentet *Regulatory Compliance and Safety Information* (Overholdelse av forskrifter og sikkerhetsinformasjon) som ble levert med denne enheten.**

Aviso **Este símbolo de aviso indica perigo. Encontra-se numa situação que lhe poderá causar danos físicos. Antes de começar a trabalhar com qualquer equipamento, familiarize-se com os perigos relacionados com circuitos eléctricos, e com quaisquer práticas comuns que possam prevenir possíveis acidentes. Para ver as traduções dos avisos que constam desta publicação, consulte o documento *Regulatory Compliance and Safety Information* (Informação de Segurança e Disposições Reguladoras) que acompanha este dispositivo.**

¡Advertencia! **Este símbolo de aviso significa peligro. Existe riesgo para su integridad física. Antes de manipular cualquier equipo, considerar los riesgos que entraña la corriente eléctrica y familiarizarse con los procedimientos estándar de prevención de accidentes. Para ver una traducción de las advertencias que aparecen en esta publicación, consultar el documento titulado *Regulatory Compliance and Safety Information* (Información sobre seguridad y conformidad con las disposiciones reglamentarias) que se acompaña con este dispositivo.**

Varning! **Denna varningssymbol signalerar fara. Du befinner dig i en situation som kan leda till personskada. Innan du utför arbete på någon utrustning måste du vara medveten om farorna med elkretsar och känna till vanligt förfarande för att förebygga skador. Se förklaringar av de varningar som förkommer i denna publikation i dokumentet *Regulatory Compliance and Safety Information* (Efterrättelse av föreskrifter och säkerhetsinformation), vilket medföljer denna anordning.**

FCC Class A Compliance

The equipment described in this document generates and may radiate radio-frequency energy. If it is not installed in accordance with Cisco installation instructions, it may cause interference with radio and television reception. This equipment has been tested and found to comply with the limits for a Class A digital device in accordance with the specifications in part 15 of the FCC rules. These specifications are designed to provide reasonable protection against such interference in a residential installation. However, there is no guarantee that interference will not occur in a particular installation.

You can determine whether your equipment is causing interference by turning it off. If the interference stops, it was probably caused by the Cisco equipment or one of its peripheral devices. If the equipment causes interference to radio or television reception, try to correct the interference by using one or more of the following measures:

- Turn the television or radio antenna until the interference stops.
- Move the equipment to one side or the other of the television or radio.
- Move the equipment farther away from the television or radio.
- Plug the equipment into an outlet that is on a different circuit from the television or radio. (That is, make certain that the equipment and the television or radio are on circuits controlled by different circuit breakers or fuses.)

Modifications to this product not authorized by Cisco Systems, Inc. could void the FCC approval and negate your authority to operate the product.

Required Tools and Equipment

Installation might require some tools and equipment that are not provided as standard equipment with the router. Following are the tools and parts required for a typical router installation:

- Number 2 Phillips screwdriver
- ESD-preventive wrist strap

Overview of Cisco 3725 AC Power Supplies

Figure 1 shows an AC power supply for the Cisco 3725 router.

Note For clarity, the AC and On/Off switch box is not shown.

Figure 2 shows the location of the power supply in the Cisco 3725 router.

Figure 1 Cisco 3725 AC Power Supply

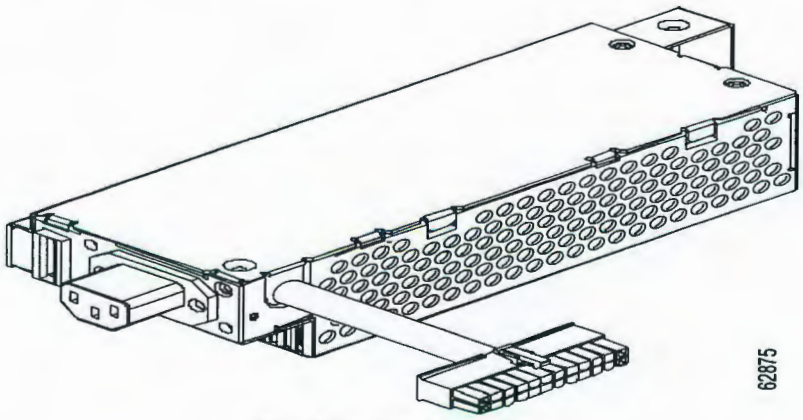
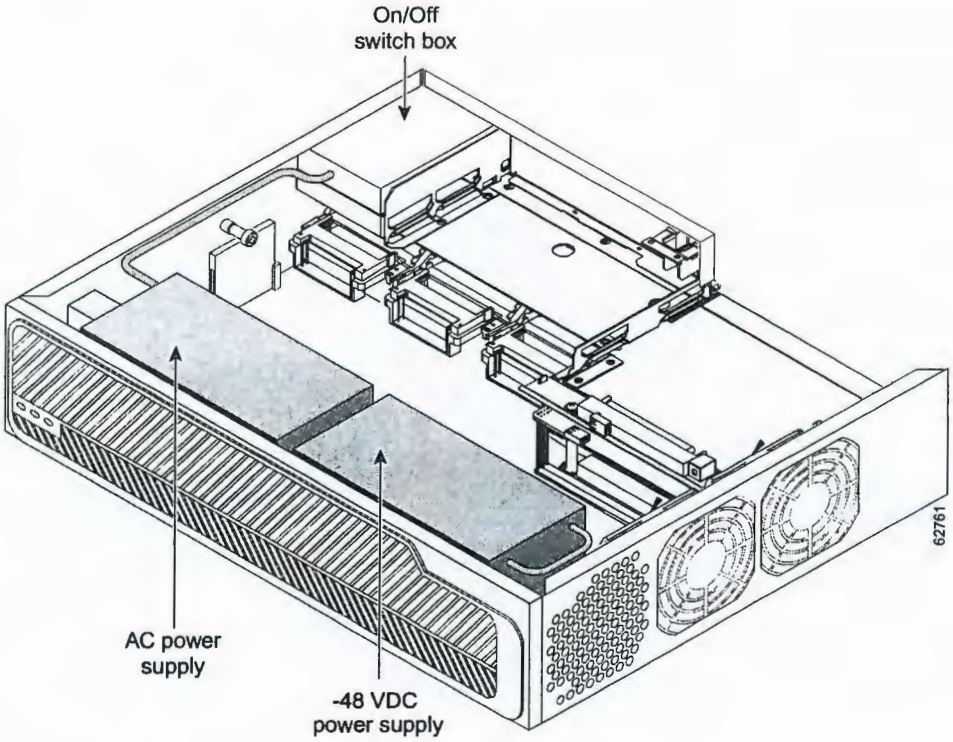


Figure 2 Power Supply Location in the Cisco 3725 Router



Accessing the Power Supply

To access power supplies on the Cisco 3725 router, remove the router cover as described in the "Removing the Router Cover" section on page 8.

Warning **Before working on a chassis or working near power supplies, unplug the power cord on AC units; disconnect the power at the circuit breaker on DC units. 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 **Do not touch the power supply when the power cord is connected. For systems with a power switch, line voltages are present within the power supply even when the power switch is off and the power cord is connected. For systems without a power switch, line voltages are present within the power supply when the power cord is connected. 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 **Do not work on the system or connect or disconnect cables during periods of lightning activity. 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 **Before opening the chassis, disconnect the telephone-network cables to avoid contact with telephone-network voltages. 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 **Network hazardous voltages are present in the BRI cable. If you detach the BRI cable, detach the end away from the router first to avoid possible electric shock. Network hazardous voltages also are present on the system card in the area of the BRI port (RJ-45 connector), regardless of when power is turned off. To see translations of the warnings that appear in this publication, refer to the *Regulatory Compliance and Safety Information* document that accompanied this device.**

Replacing the Cisco 3725 Power Supply

The power supply and cabling for the Cisco 3725 router is contained inside the chassis. To replace the power supply, complete these procedures:

- Removing the Router Cover, page 8
- Removing the Cisco 3725 Power Supply, page 9
- Installing the Cisco 3725 Power Supply, page 15
- Replacing the Router Cover, page 16

Removing the Router Cover

To gain access to the Cisco 3725 power supply, you must first remove the chassis cover:

Step 1 Turn off power to the router.

Step 2 Remove all network interface cables from the rear panel.

Step 3 Remove the power cord.

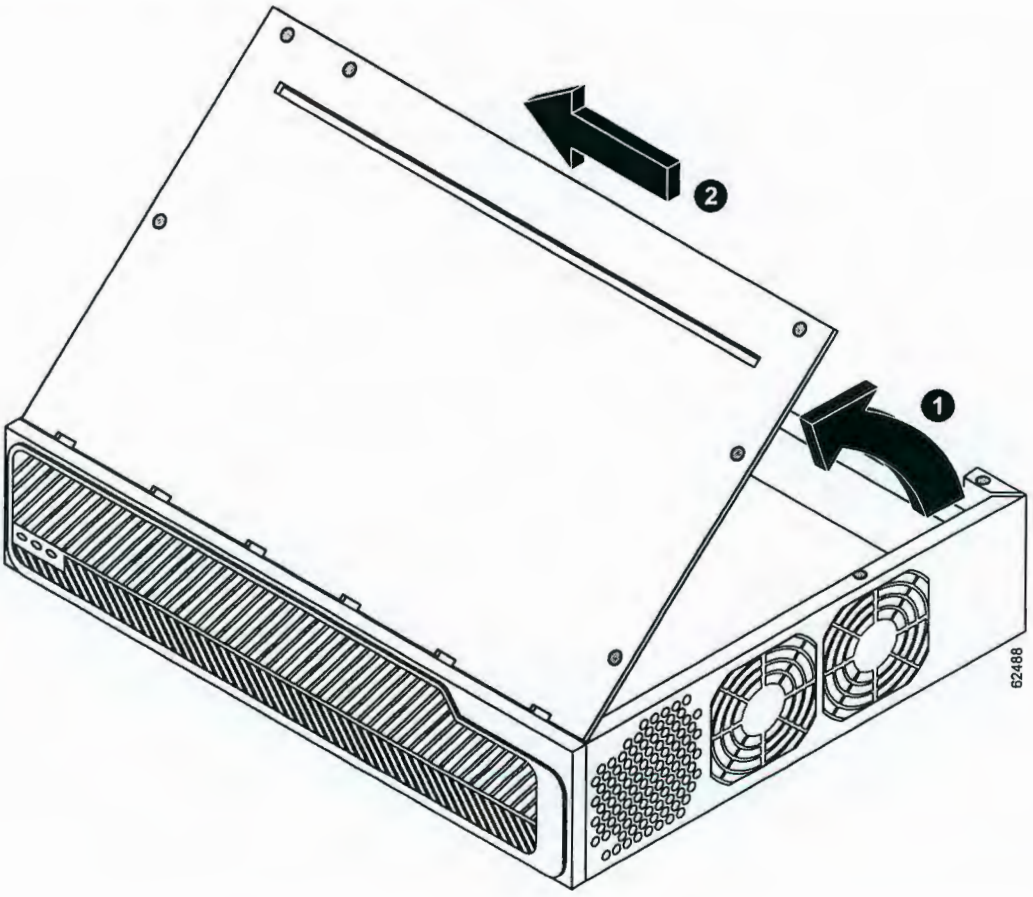
Warning **When installing the unit, always make the ground connection first and disconnect it last. To see translations of the warnings that appear in this publication, refer to the *Regulatory Compliance and Safety Information* document that accompanied this device.**

Step 4 Place the router so the rear panel is closest to you. Remove the six screws located on top of the cover. Set the screws aside in a safe place.

Step 5 Lift the front edge of the cover. (See number 1 in Figure 3.)

Step 6 Slide the cover toward the right until the metal tabs on the rear edge separate from the chassis bottom. (See number 2 in Figure 3.)

Figure 3 Removing the Cisco 3725 Cover



Step 7 Lift the cover completely off and set it aside.

When you are ready to replace the cover, see the "Replacing the Router Cover" section on page 16.

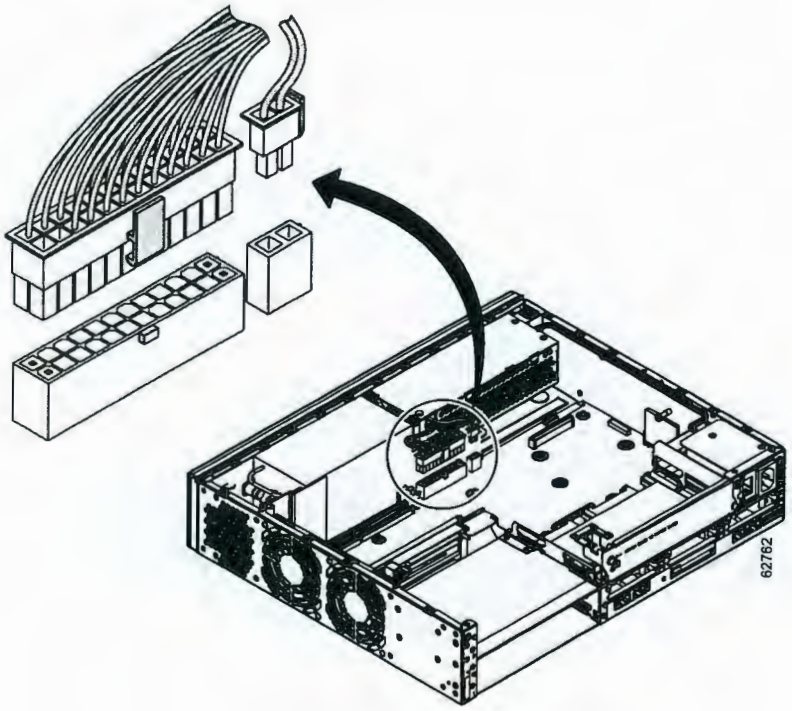
Removing the Cisco 3725 Power Supply

After you remove the cover from the chassis, follow this procedure to remove the power supply:

Step 1 Find the large and small power connectors on the motherboard and remove them. (See Figure 4.)

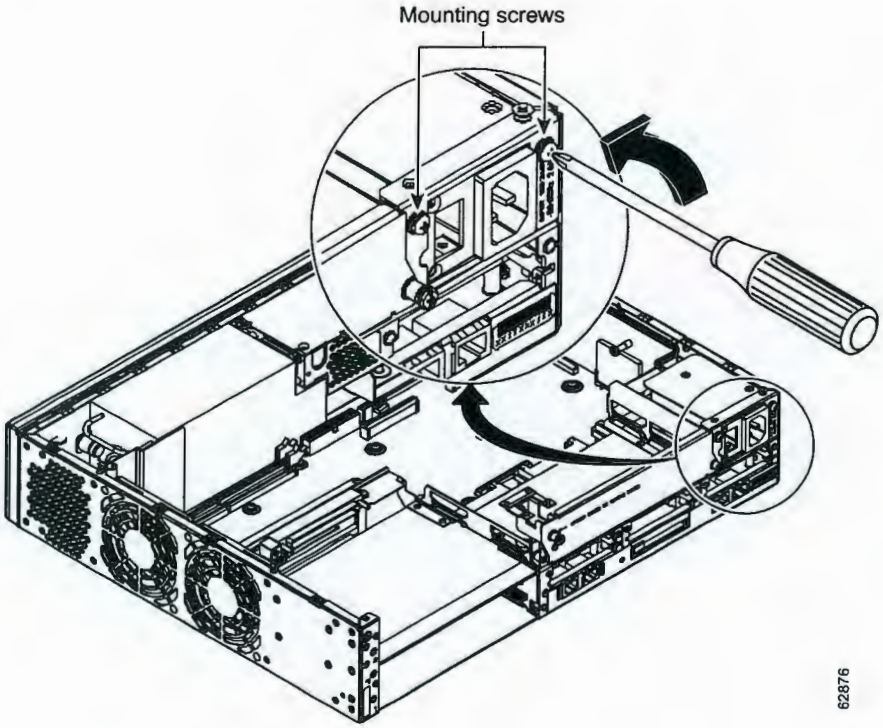
Note On a Cisco 3725 router, you can simply lift the connector away from the receptacle. (See Figure 4.)

Figure 4 Removing the Cisco 3725 Power Connectors



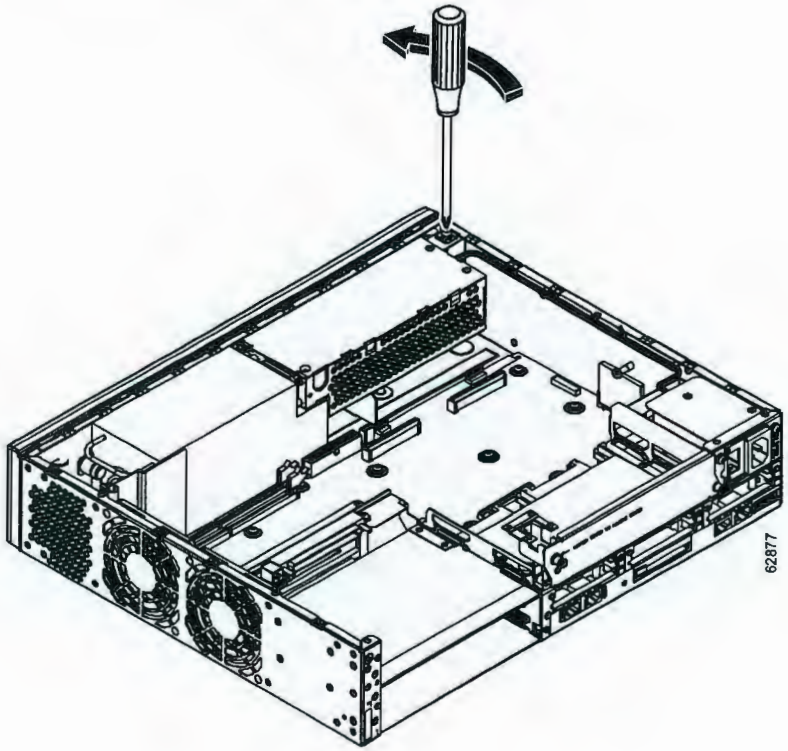
Step 2 The Cisco 3725 power supply connector is held in the chassis by two external mounting screws at the rear of the router. (See Figure 5.) Remove the screws and set them aside.

Figure 5 Cisco 3725 Power Supply Connector Mounting Screws



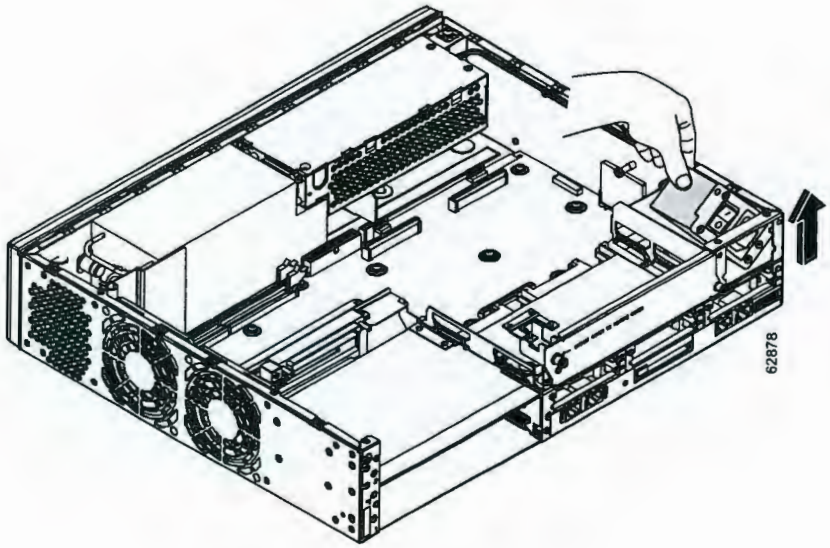
Step 3 The Cisco 3725 power supply is held in the chassis by one top-level screw towards the front and left side of the router. (See Figure 6.) Remove the screw and set it aside.

Figure 6 Cisco 3725 Power Supply Mounting Screw



Step 4 Lift the power supply On/Off switch box, at an angle, up and out of the chassis. (See Figure 7.)

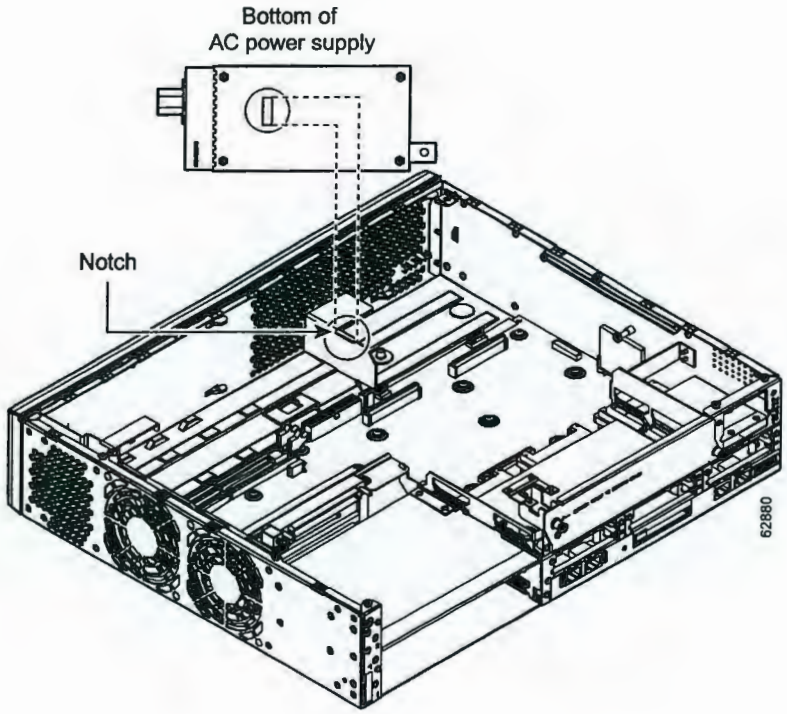
Figure 7 Cisco 3725 Power Supply Mounting Hinge (Right)



Step 5 Slide the power supply back slightly in the chassis. This disengages the hooks built into the chassis that help secure the power supply. (See Figure 8.)

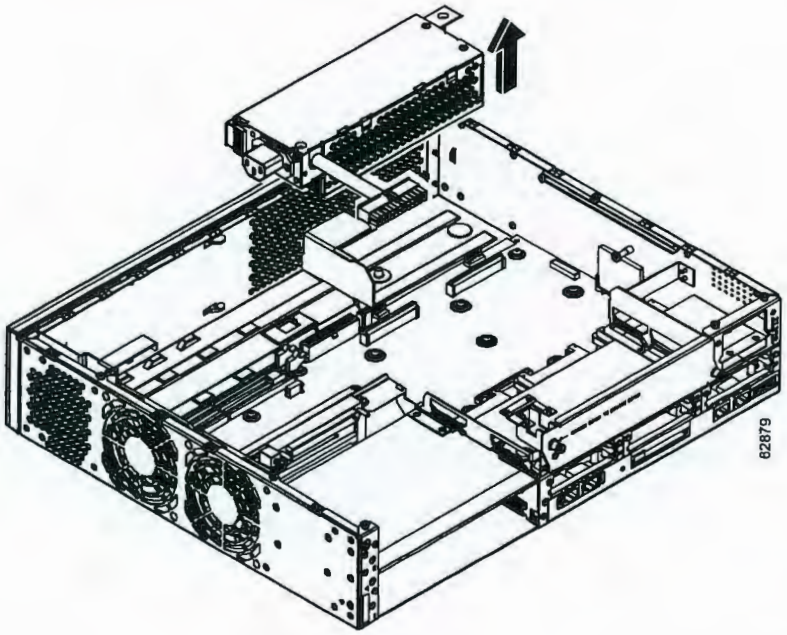
Note The DC power supply cannot be present when removing the AC power supply.

Figure 8 Cisco 3725 Power Supply Hinge Disengagement



Step 6 Pull the power supply back and lift the power supply out of the chassis. (See Figure 9.)

Figure 9 Removing the Cisco 3725 Power Supply from the Chassis



Installing the Cisco 3725 Power Supply

Follow these steps to install a power supply in the chassis:

Step 1 Place the power supply in the chassis, with the power supply rear panel slightly separated from the chassis rear panel. This position allows the hook in the chassis to engage the cutout in the bottom of the power supply. (See Figure 8.)

Step 2 Slide the power supply toward the side of the chassis, engaging the hook in the chassis. This enables the power supply to drop and engage the hinge preventing further movement.

Step 3 Replace the top-level mounting screw that holds the power supply in place. (See Figure 6.)

Step 4 Replace the power supply connectors and the external connector mounting screws at the rear of the chassis. (See Figure 5.)

Step 5 Insert the large power connector into the receptacle on the motherboard. (See Figure 4.)

Replacing the Router Cover

After you finish replacing the power supply, follow these steps to replace the cover:

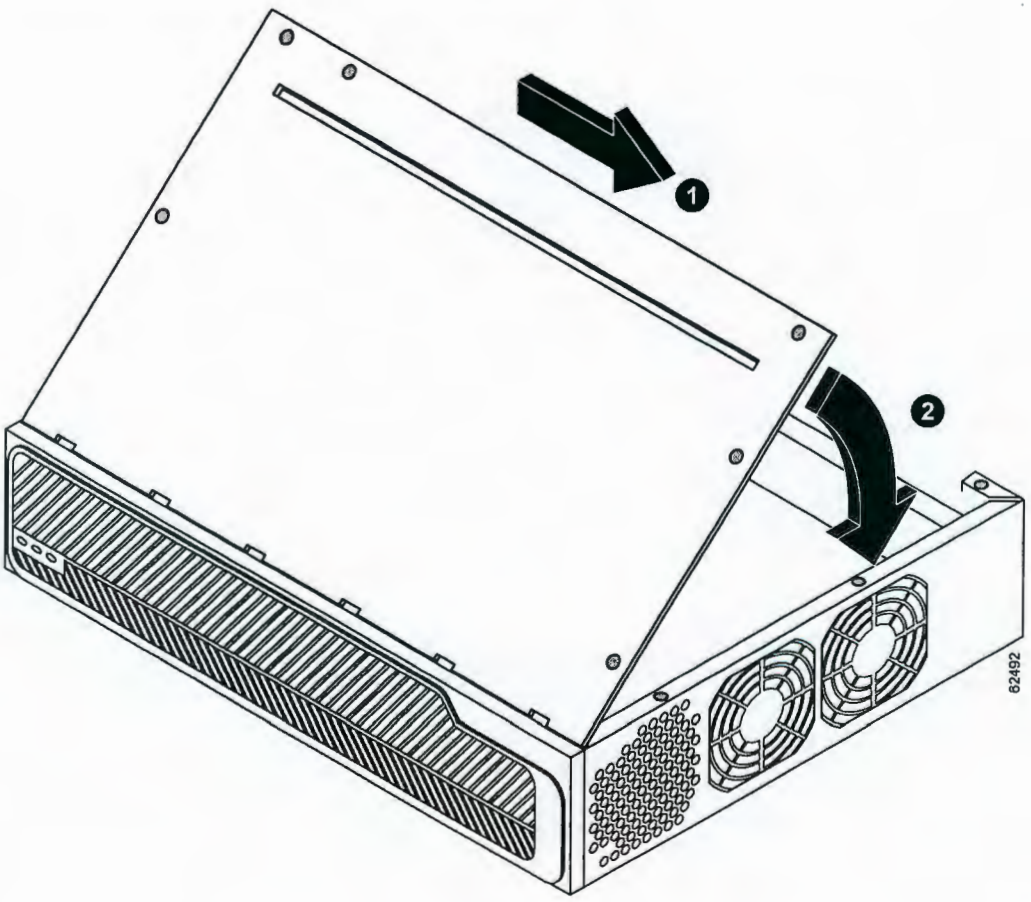
Step 1 Place the chassis bottom so the front panel is closest to you.

Step 2 Hold the cover so the tabs at the rear of the cover are aligned with the chassis bottom.

Step 3 Push the cover toward the rear, making sure that the cover tabs fit under the chassis back panel, and the back panel tabs fit under the cover.

Step 4 Slide the cover slightly to the left to lock the cover into position (number 1 in Figure 10).

Figure 10 Replacing the Cisco 3725 Router Cover



Step 5 Lower the front of the cover onto the chassis (number 2 in Figure 10).

Step 6 Fasten the cover with the five screws you set aside earlier.

Step 7 Reinstall the chassis on a rack.

Step 8 Reinstall network interface cables.

Step 9 Proceed to the "Electrical Connections for Cisco 3725 Routers" section on page 17.

Electrical Connections for Cisco 3725 Routers

This section explains how to connect AC power to Cisco 3725 routers.

Warning **This unit is intended for installation in restricted access areas. A restricted access area is where access can only be gained by service personnel through the use of a special tool, lock and key, or other means of security, and is controlled by the authority responsible for the location. 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 **Before performing any of the following procedures, ensure that power is OFF. To see translations of the warnings that appear in this publication, refer to the *Regulatory Compliance and Safety Information* document that accompanied this device.**

Note The installation must comply with the 1996 National Electric Code (NEC) and other applicable codes.

Note Use copper conductors only.

Powering On the Router

Warning **The plug-socket combination must be accessible at all times because it serves as the main disconnecting device. To see translations of the warnings that appear in this publication, refer to the *Regulatory Compliance and Safety Information* document that accompanied this device.**

Caution Never operate the router unless the unit is completely closed, to ensure adequate cooling.

Take the following steps to power on the router:

Step 1 For routers with AC input, plug the router's power cord into a three-terminal, single-phase power source that provides power within the acceptable range.

Step 2 Power on the router. The LED labeled SYSTEM on the front panel should come on.

If you encounter problems when you power on the router, see the "Troubleshooting" section that follows.

Troubleshooting

Check the following items to help isolate problems with the power supply installation:

- With the power switch on, is the power LED on the front panel on?
  - If not, check the AC or DC input, AC or DC source, router circuit breaker, and the power supply cable (AC) or power supply wiring (DC).
  - Check the power supply connection to the motherboard.
  - If the power LED is still off, the problem might be a power supply failure.
- Does the router shut down after being on a short time?
  - Check the fans. If the fans are not working, the router will overheat and shut itself down.
  - If the fans are not working, check the power supply connections to the fans.
  - Ensure that the chassis intake and exhaust vents are clear.
  - Check the environmental site requirements in your router installation and configuration 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_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
- 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.

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.

Preparing to Install the Router

This chapter describes site requirements and equipment needed to install your Cisco 3700 series router. It includes the following sections:

After you have completed this chapter, proceed to Chapter 3, "Installing the Router" for installation instructions.

Safety Recommendations

Follow these guidelines to ensure general safety:

- Keep the chassis area clear and dust-free during and after installation.
- If you remove the chassis cover, put it in a safe place.
- Keep tools and chassis components away from walk areas.
- Do not wear loose clothing that could get caught in the chassis. Fasten your tie or scarf and roll up your sleeves.
- Wear safety glasses when working under conditions that might be hazardous to your eyes.
- Do not perform any action that creates a hazard to people or makes the equipment unsafe.

Safety with Electricity

Follow these guidelines when working on equipment powered by electricity:

Warning **Read the installation instructions before connecting the system to the power source. To see translations of the warnings that appear in this publication, refer to the *Regulatory Compliance and Safety Information* document that accompanied this device.**

- Locate the emergency power-off switch in the room in which you are working. Then, if an electrical accident occurs, you can quickly turn off the power.
- Disconnect all power before doing the following:
  - Installing or removing a chassis
  - Working near power supplies
- Look carefully for possible hazards in your work area, such as moist floors, ungrounded power extension cables, frayed power cords, and missing safety grounds.
- Do not work alone if hazardous conditions exist.
- Never assume that power is disconnected from a circuit. Always check.
- If an electrical accident occurs, proceed as follows:
  - Use caution; do not become a victim yourself.
  - Turn off power to the device.
  - If possible, send another person to get medical aid. Otherwise, assess the victim's condition and then call for help.
  - Determine if the person needs rescue breathing or external cardiac compressions; then take appropriate action.

In addition, use the following guidelines when working with any equipment that is disconnected from a power source, but still connected to telephone wiring or other network cabling:

- Never install telephone wiring during a lightning storm.
- Never install telephone jacks in wet locations unless the jack is specifically designed for it.
- Never touch uninsulated telephone wires or terminals unless the telephone line is disconnected at the network interface.
- Use caution when installing or modifying telephone lines.

Preventing Electrostatic Discharge Damage

Electrostatic discharge (ESD) can damage equipment and impair electrical circuitry. It can occur if electronic printed circuit cards are improperly handled and can cause complete or intermittent failures. Always follow ESD prevention procedures when removing and replacing modules:

- Ensure that the router chassis is electrically connected to earth ground.
- Wear an ESD-preventive wrist strap, ensuring that it makes good skin contact. Connect the clip to an unpainted surface of the chassis frame to channel unwanted ESD voltages safely to ground. To guard against ESD damage and shocks, the wrist strap and cord must operate effectively.
- If no wrist strap is available, ground yourself by touching a metal part of the chassis.

Caution For the safety of your equipment, periodically check the resistance value of the antistatic strap. It should be between 1 and 10 megohms (Mohm).

General Site Requirements

This section describes the requirements your site must meet for safe installation and operation of your router. Ensure that the site is properly prepared before beginning installation. If you are experiencing shutdowns or unusually high errors with your existing equipment, this section can also help you isolate the cause of failures and prevent future problems.

Power Supply Considerations

Check the power at your site to ensure that you are receiving "clean" power (free of spikes and noise). Install a power conditioner if necessary.

Warning **The device is designed for connection to TN and IT power systems. To see translations of the warnings that appear in this publication, refer to the *Regulatory Compliance and Safety Information* document that accompanied this device.**

The AC power supply includes the following features:

- Autoselects either 110 V or 220 V operation.
- All units include a 6-foot (1.8-meter) electrical power cord. (A label near the power cord indicates the correct voltage, frequency, current draw, and power dissipation for the unit.)

Table 2-1 lists power requirements for Cisco 3700 series routers.

Table 2-1 Power Requirements for Cisco 3700 Series Routers

Router	Power Supply	Input Power	Input Voltage Tolerance Limits
Cisco 3725	AC	100 - 240 VAC, 10.0 A, 50 - 60 Hz	85 - 264 VAC
	DC, nominal 24/48 VDC	24 - 36 VDC, 9 A, positive or negative input, single or dual sources	18 - 72 VDC
		36 - 60 VDC, 4 A, positive or negative input, single or dual sources	
Cisco 3745	AC	100 - 240 VAC, 10.0 A, 50 - 60 Hz	85 - 264 VAC
	DC, nominal 24/48 VDC	24 - 36 VDC, 15 A, positive or negative input	18 - 72 VDC
		36 - 60 VDC, 7 A, positive or negative input	
	DC, nominal 48 VDC	48 - 60 VDC, 10 A, positive or negative input	38 - 72 VDC

Site Environment

Cisco 3700 series routers can be placed on a desktop or installed in a rack. The location of your router and the layout of your equipment rack or wiring room are extremely important considerations for proper operation. Equipment placed too close together, inadequate ventilation, and inaccessible panels can cause malfunctions and shutdowns, and can make maintenance difficult. Plan for access to both front and rear panels of the router.

When planning your site layout and equipment locations, remember the precautions described in the next section "Site Configuration" to help avoid equipment failures and reduce the possibility of environmentally caused shutdowns. If you are currently experiencing shutdowns or an unusually high number of errors with your existing equipment, these precautions may help you isolate the cause of the failures and prevent future problems.

Site Configuration

The following precautions will help you plan an acceptable operating environment for your router and will help you avoid environmentally caused equipment failures:

- Ensure that the room where your router operates has adequate circulation. Electrical equipment generates heat. Without adequate circulation, ambient air temperature may not cool equipment to acceptable operating temperatures.
- Always follow ESD-prevention procedures described in the "Preventing Electrostatic Discharge Damage" section on page 2-2 to avoid damage to equipment. Damage from static discharge can cause immediate or intermittent equipment failure.
- Ensure that the chassis cover or mainboard tray and module rear panels are secure. All empty network module slots, interface card slots, and power supply bays must have filler panels installed. The chassis is designed to allow cooling air to flow within it, through specially designed cooling slots. A chassis with uncovered openings will create air leaks, which may interrupt and reduce the flow of air across internal components.

Equipment Racks

Cisco 3700 series routers include brackets for use with a 19-inch rack or, if specified in your order, optional larger brackets for use with a 23-inch rack.

The following information will help you plan your equipment rack configuration:

- Allow clearance around the rack for maintenance.
- Enclosed racks must have adequate ventilation. Ensure that the rack is not congested, because each router generates heat. An enclosed rack should have louvered sides and a fan to provide cooling air. Heat generated by equipment near the bottom of the rack can be drawn upward into the intake ports of the equipment above.
- When mounting a chassis in an open rack, ensure that the rack frame does not block the intake ports or exhaust ports. If the chassis is installed on slides, check the position of the chassis when it is seated into the rack.
- Baffles can help to isolate exhaust air from intake air, which also helps to draw cooling air through the chassis. The best placement of the baffles depends on the airflow patterns in the rack, which can be found by experimenting with different configurations.

- When equipment installed in a rack (particularly in an enclosed rack) fails, try operating the equipment by itself, if possible. Power OFF other equipment in the rack (and in adjacent racks) to allow the router under test a maximum of cooling air and clean power.

Installation Checklist

The sample installation checklist lists items and procedures for installing a new router. Make a copy of this checklist and mark the entries when completed. Include a copy of the checklist for each router in your Site Log (described in the next section, "Creating a Site Log").

Installation checklist for site_____

Router name_____

Task	Verified by	Date
Installation Checklist copied		
Background information placed in Site Log		
Site power voltages verified		
Installation site power check completed		
Required tools available		
Additional equipment available		
Router received		
Router quick start guide received		
Cisco 2600 Series, Cisco 3600 Series, and Cisco 3700 Series Regulatory Compliance and Safety Information document received		
Optional ordered printed documentation and documentation CD-ROM received		
Cisco Information Packet received		
Chassis components verified		
Initial electrical connections established		
ASCII terminal (for local configuration) or modem (for remote configuration) available		
Signal distance limits verified		
Startup sequence steps completed		
Initial operation verified		
Software image verified		

Creating a Site Log

The Site Log provides a record of all actions related to the router. Keep it in an accessible place near the chassis where anyone who performs tasks has access to it. Use the Installation Checklist to verify steps in the installation and maintenance of the router. Site Log entries might include the following information:

- Installation progress—Make a copy of the Installation Checklist and insert it into the Site Log. Make entries as each procedure is completed.
- Upgrade and maintenance procedures—Use the Site Log as a record of ongoing router maintenance and expansion history. A Site Log might include the following events:
  - Installation of network modules
  - Removal or replacement of network modules and other upgrades
  - Configuration changes
  - Maintenance schedules and requirements
  - Maintenance procedures performed
  - Intermittent problems
  - Comments and notes

Inspecting the Router

Do not unpack the router until you are ready to install it. If the final installation site will not be ready for some time, keep the chassis in its shipping container to prevent accidental damage. When you are ready to install the router, proceed with unpacking it.

The router, cables, publications, and any optional equipment you ordered may be shipped in more than one container. When you unpack the containers, check the packing list to ensure that you received all the following items:

- Router
- 6-foot (1.8-meter) power cord
- Rubber feet for desktop mounting
- Rack-mount brackets
- Ground lug
- Cable guides (for Cisco 3725 routers)
- RJ-45-to-DB-9 adapter cable
- RJ-45-to-DB-25 adapter cable
- Optional equipment (such as network connection cables or additional rack-mount brackets)
- *Cisco 3725 Router Quick Start Guide*, if applicable
- *Cisco 3745 Router Quick Start Guide*, if applicable
- *Cisco 2600 Series, Cisco 3600 Series, and Cisco 3700 Series Regulatory Compliance and Safety Information* document

Inspect all items for shipping damage. If anything appears to be damaged, or if you encounter problems installing or configuring your router, contact customer service. Warranty, service, and support information is in the quick start guide that shipped with your router.

Required Tools and Equipment for Installation and Maintenance

You need the following tools and equipment to install and upgrade the router and its components:

- ESD-preventive cord and wrist strap
- Number 2 Phillips screwdriver
- Flat-blade screwdrivers: small, 3/16-in. (0.476 cm) and medium, 1/4-in. (0.625 cm)
  - To install or remove modules
  - To remove the cover or mainboard tray, if you are upgrading memory or other components
- Screws that fit your rack
- Wire crimper
- AWG 6 (13 mm^2) wire to connect the router chassis to earth ground

In addition, depending on the type of modules you plan to use, you might need the following equipment to connect a port to an external network:

- Cables for connection to the WAN and LAN ports (dependent on configuration)

Note For more information on cable specifications, refer to the online document *Cisco Modular Access Router Cable Specifications* located both on Cisco.com and on the Documentation CD-ROM that accompanied your router.

- Ethernet hub or PC with a network interface card for connection to the Ethernet (LAN) port(s).
- Console terminal (an ASCII terminal or a PC running terminal emulation software) configured for 9600 baud, 8 data bits, no parity, and 2 stop bits.
- Modem for connection to the auxiliary port for remote administrative access (optional).
- Token Ring media attachment unit (MAU) for any Token Ring interfaces installed in your router.
- Data service unit (DSU) or channel service unit/data service unit (CSU/DSU) as appropriate for serial interfaces.
- External CSU for any CT1/PRI modules without a built-in CSU.
- NT1 device for ISDN BRI S/T interfaces (if not supplied by your service provider).

Console and Auxiliary Port Considerations

The router includes an asynchronous serial console port and an auxiliary port. The console and auxiliary ports provide access to the router either locally using a console terminal connected to the console port, or remotely using a modem connected to the auxiliary port. This section discusses important cabling information to consider before connecting the router to a console terminal or modem.

The main difference between the console and auxiliary ports is that the auxiliary port supports hardware flow control and the console port does not. Flow control paces the transmission of data between a sending device and a receiving device. Flow control ensures that the receiving device can absorb the data sent to it before the sending device sends more. When the buffers on the receiving device are full, a message is sent to the sending device to suspend transmission until the data in the buffers has been processed. Because the auxiliary port supports flow control, it is ideally suited for use with the high-speed transmissions of a modem. Console terminals send data at slower speeds than modems; therefore, the console port is ideally suited for use with console terminals.

Console Port Connections

The router has an EIA/TIA-232 asynchronous serial console port (RJ-45). Depending on the cable and the adapter used, this port will appear as a DTE or DCE device at the end of the cable.

For connection to a PC running terminal emulation software, your router is provided with an RJ-45 to DB-9 adapter cable.

To connect the router to an ASCII terminal, use an RJ-45 rollover cable and an RJ-45-to-DB-25 female adapter (not provided).

The default parameters for the console port are 9600 baud, 8 data bits, no parity, and 2 stop bits. The console port does not support hardware flow control. For detailed information about installing a console terminal, see the "Connecting to a Console Terminal or Modem" section on page 3-19.

For cable and port pinouts, refer to the online document *Cisco Modular Access Router Cable Specifications*. This document is located on Cisco.com and on the Documentation CD-ROM that accompanied your router.

Auxiliary Port Connections

The router has an EIA/TIA-232 asynchronous serial auxiliary port (RJ-45) that supports flow control. Depending on the cable and the adapter used, this port will appear as a DTE or DCE device at the end of the cable.

For connection to a modem, your router is provided with an RJ-45-to-DB-25 adapter cable.

For detailed information about connecting devices to the auxiliary port, see the "Connecting to a Console Terminal or Modem" section on page 3-19.

For cable and port pinouts, refer to the *Cisco Modular Access Router Cable Specifications* document online or on the Documentation CD-ROM.

Preparing to Connect to a Network

When setting up your router, consider distance limitations and potential electromagnetic interference (EMI) as defined by the applicable local and international regulations.

Network connection considerations are provided for several types of network interfaces and are described in the following sections:

Refer to the following online documents for more information about network connections and interfaces:

- *Cisco Network Modules Hardware Installation Guide*
- *Cisco Interface Cards Installation Guide*
- *Cisco Modular Access Router Cable Specifications*

Warning **To avoid electric shock, do not connect safety extra-low voltage (SELV) circuits to telephone-network voltage (TNV) circuits. LAN ports contain SELV circuits, and WAN ports contain TNV circuits. Some LAN and WAN ports both use RJ-45 connectors. To see translations of the warnings that appear in this publication, refer to the *Regulatory Compliance and Safety Information* document that accompanied this device.**

Ethernet Connections

The IEEE has established Ethernet as standard IEEE 802.3. The most common Ethernet implementations are as follows:

- 100BASE-T—2-pair Category 5 or unshielded twisted-pair (UTP) straight-through RJ-45 cable.
- 10BASE-2—Ethernet on thin coaxial cable, also known as thin Ethernet. The maximum segment distance is 607 feet (186 meters).
- 10BASE-5—Ethernet on thick coaxial cable, also known as thick Ethernet. The maximum segment distance is 1,640 feet (500 meters).
- 10BASE-T—Ethernet on unshielded twisted-pair (UTP) cable. The maximum segment distance is 328 feet (100 meters). UTP cables look like the wiring used for ordinary telephones; however, UTP cables meet certain electrical standards that telephone cables do not meet.

Refer to the *Cisco Modular Access Router Cable Specifications* online document for information about Ethernet cables, connectors, and pinouts. This document is available online and on the Cisco Documentation CD-ROM.

Token Ring Connections

The IEEE has established Token Ring as standard IEEE 802.5. Specifications indicate a maximum segment distance of 328 feet (100 meters) for UTP cabling.

Note To ensure agency compliance with FCC Class B electromagnetic emissions requirements (EMI), make sure that you use a shielded RJ-45 Token Ring cable when connecting your router to a Token Ring network.

Token Ring can operate at two different ring speeds: 4 and 16 Mbps. All devices on the Token Ring must use the same operating speed.

Use a Token Ring cable to connect the router to a switch. Refer to the section "Token Ring Port Pinouts" in the *Cisco Modular Access Router Cable Specifications* online document for the Token Ring port pinouts. This document is available online and on the Cisco Documentation CD-ROM.

Serial Connections

Serial connections are provided by WAN interface cards and network modules. For more information on WAN interface cards, refer to the *Cisco Interface Cards Installation Guide*. For more information on network modules, refer to the *Cisco Network Modules Hardware Installation Guide*. These documents are accessible online and on the Cisco Documentation CD-ROM.

Before you connect a device to a serial port, you need to know the following:

- Type of device, data terminal equipment (DTE) or data communications equipment (DCE), you are connecting to the synchronous serial interface
- Type of connector, male or female, required to connect to the device
- Signaling standard required by the device

Configuring Serial Connections

The serial ports on the asynchronous/synchronous serial network modules and the serial WAN interface card use DB-60 connectors. Serial ports can be configured as DTE or DCE, depending on the serial cable used.

Serial DTE or DCE Devices

A device that communicates over a synchronous serial interface is either a DTE or DCE device. A DCE device provides a clock signal that paces the communications between the device and the router. A DTE device does not provide a clock signal. DTE devices usually connect to DCE devices. The documentation that accompanied the device should indicate whether it is a DTE or DCE device. (Some devices have a jumper to select either DTE or DCE mode.) Table 2-2 lists typical DTW and DCE devices.

Table 2-2 Typical DTE and DCE Devices

Device Type	Gender	Typical Devices
DTE	Male[1]	Terminal PC
DCE	Female[2]	Modem CSU/DSU Multiplexer

1. If pins protrude from the base of the connector, the connector is male.
2. If the connector has holes to accept pins, the connector is female.

Signaling Standards Supported

The synchronous serial ports available for the router support the following signaling standards: EIA/TIA-232, EIA/TIA-449, V.35, X.21, and EIA-530. You can order a Cisco DB-60 shielded serial transition cable that has the appropriate connector for the standard you specify. The documentation for the device you want to connect should indicate the standard used for that device. The router end of the shielded serial transition cable has a DB-60 connector, which connects to the DB-60 port on a serial WAN interface card. The other end of the serial transition cable is available with a connector appropriate for the standard you specify.

The synchronous serial port can be configured as DTE or DCE, depending on the attached cable (except EIA-530, which is DTE only). To order a shielded cable, contact customer service. See the "Obtaining Technical Assistance" section on page xvii.

Note All serial ports configured as DTE require external clocking from a CSU/DSU or other DCE device.

Although manufacturing your own serial cables is not recommended (because of the small size of the pins on the DB-60 serial connector), cable pinouts are provided in the *Cisco Modular Access Router Cable Specifications* document.

Distance Limitations

Serial signals can travel a limited distance at any given bit rate; generally, the slower the data rate, the greater the distance. All serial signals are subject to distance limits, beyond which a signal significantly degrades or is completely lost.

Note Only the serial WAN interface card supports bit rates above 128 Kbps.

Table 2-3 lists the recommended maximum speeds and distances for each serial interface type; however, you might get good results at speeds and distances greater than those listed, if you understand the electrical problems that might arise and can compensate for them. For instance, the recommended maximum rate for V.35 is 2 Mbps, but 4 Mbps is commonly used.

Table 2-3 Serial Signal Transmission Speeds and Distances

Rate (bps)	EIA/TIA-232 Distance		EIA/TIA-449, X.21, V.35, EIA-530 Distance	
	Feet	Meters	Feet	Meters
2400	200	60	4100	1250
4800	100	30	2050	625
9600	50	15	1025	312
19200	25	7.6	513	156
38400	12	3.7	256	78
56000	8.6	2.6	102	31
1544000 (T1)	—	—	50	15

Balanced drivers allow EIA/TIA-449 signals to travel greater distances than EIA/TIA-232 signals. The recommended distance limits for EIA/TIA-449 shown in Table 2-3 are also valid for V.35, X.21, and EIA-530. Typically, EIA/TIA-449 and EIA-530 can support 2-Mbps rates, and V.35 can support 4-Mbps rates.

Asynchronous/Synchronous Serial Module Baud Rates

The following baud-rate limitations apply to the slow-speed serial interfaces found in the asynchronous/synchronous serial modules:

- Asynchronous interface—Maximum baud rate is 115.2 kbps.
- Synchronous interface—Maximum baud rate is 128-kbps full duplex.

ISDN BRI Connections

The BRI WAN interface cards provide Integrated Services Digital Network (ISDN) Basic Rate Interface (BRI) connections. The BRI modules and BRI WAN interface cards are available with either an S/T interface that requires an external Network Terminator 1 (NT1), or a U interface that has a built-in NT1.

You can install the BRI modules in any available slot in the chassis.

Warning **Hazardous network voltages are present in WAN ports regardless of whether power to the unit is OFF or ON. To avoid electric shock, use caution when working near WAN ports. When detaching cables, detach the end away from the unit first. To see translations of the warnings that appear in this publication, refer to the *Regulatory Compliance and Safety Information* document that accompanied this device.**

Use a BRI cable (not included) to connect the BRI WAN interface card directly to an ISDN. Table 2-4 lists the specifications for ISDN BRI cables. Also, refer to the *Cisco Modular Access Router Cable Specifications* online document for pinouts. This document is located on Cisco.com and the Documentation CD-ROM.

Table 2-4 ISDN BRI Cable Specifications

Specification	High-Capacitance Cable	Low-Capacitance Cable
Resistance (at 96 kHz)	160 ohms/km	160 ohms/km
Capacitance (at 1 kHz)	120 nF[1]/km	30 nF/km
Impedance (at 96 kHz)	75 ohms	150 ohms
Wire diameter	0.024 in. (0.6 mm)	0.024 in. (0.6 mm)
Distance limitation	32.8 ft (10 m)	32.8 ft (10 m)

1. nF = nanoFarad

For more information on BRI WAN interface cards, refer to the *Cisco Interface Cards Installation Guide* online document. This document is located on Cisco.com and the Documentation CD-ROM.

56-K/Switched-56-kbps DSU/CSU Connections

Switched-56-kbps connections are provided by the 56-kbps DSU/CSU WAN interface card.

For more information on Switched-56-kbps WAN interface cards, refer to the *Cisco Interface Cards Installation Guide* online document. This document is located on Cisco.com and the Documentation CD-ROM.

Overview of Cisco Network Modules

This chapter provides an overview of Cisco network modules used in Cisco modular access routers. It is organized by router:

Cisco 2600 Series Routers

Table 1-1 lists network module options available for Cisco 2600 series routers.

Note References to the Cisco 2600 series apply to all of the following routers: Cisco 2610, Cisco 2610XM, Cisco 2611, Cisco 2611XM, Cisco 2612, Cisco 2613, Cisco 2620, Cisco 2620XM, Cisco 2621, Cisco 2621XM, Cisco 2650, Cisco 2650XM, Cisco 2651, Cisco 2651XM, and Cisco 2691.

Note References to the Cisco 2600XM routers apply to the following routers: Cisco 2610XM, Cisco 2611XM, Cisco 2620XM, Cisco 2621XM, Cisco 2650XM, and Cisco 2651XM.

Table 1-1 Network Module Options for Cisco 2600 Series Routers

Network Module		Supported in Cisco IOS Releases:		
Description	Product Number	Specific Limited Lifetime	First "T" (Technology)	First Mainline
1-Port Ethernet	NM-1E	–	11.3(4)T	12.0(1)
4-Port Ethernet	NM-4E	–	11.3(4)T	12.0(1)
4- or 8-Port Asynchronous/Synchronous Serial	NM-4A/S NM-8A/S	11.3(2)XA	11.3(3)T	12.0(1)
16-Port Asynchronous/Synchronous Serial[1]	NM-16A/S	12.2(15)ZJ	–	–
16- or 32-Port Asynchronous Serial	NM-16A NM-32A	11.3(2)XA	11.3(3)T	12.0(1)
1- or 2-Slot Voice	NM-1V NM-2V	11.3(2)XA	11.3(3)T	12.0(1)
1- or 2-Slot Voice[1]	NM-HD-1V NM-HD-2V NM-HD-2VE	12.2(15)ZJ	–	–
4- or 8-Port ISDN BRI with S/T interface	NM-4B-S/T NM-8B-S/T	–	11.3(4)T	12.0(1)
4- or 8-Port ISDN BRI with U interface	NM-4B-U NM-8B-U	–	11.3(4)T	12.0(1)
1- or 2-Port Channelized T1/ISDN PRI	NM-1CT1 NM-2CT1	–	11.3(4)T	12.0(1)
1- or 2-Port Channelized T1/ISDN PRI with CSU	NM-1CT1-CSU NM-2CT1-CSU	–	11.3(4)T	12.0(1)
1- or 2-Port Channelized E1/ISDN PRI Unbalanced	NM-1CE1U NM-2CE1U	–	11.3(4)T	12.0(1)
1- or 2-Port Channelized E1/ISDN PRI Balanced	NM-1CE1B NM-2CE1B	–	11.3(4)T	12.0(1)

Table 1-1 Network Module Options for Cisco 2600 Series Routers (continued)

Network Module		Supported in Cisco IOS Releases:		
Description	Product Number	Specific Limited Lifetime	First "T" (Technology)	First Mainline
1- or 2-Port T1/E1 Channelized PRI with G.703[2]	NM-1CE1T1-PRI NM-2CE1T1-PRI	–	12.3T	–
8- or 16-Port Analog Modem	NM-8AM NM-16AM	–	11.3(4)T	12.0(1)
1-Port ATM-25	NM-1ATM-25	–	11.3(4)T	12.0(1)
1-Port ATM T3/E3	NM-1A-T3 NM-1A-E3	–	12.1(2)T	–
4- or 8-Port T1/E1 IMA	NM-4T1-IMA NM-4E1-IMA NM-8T1-IMA NM-8E1-IMA	–	12.0(5)T	–
High-Density Voice	NM-HDV	–	12.0(6)T	–
2-Slot WAN	NM-2W	12.0(7)XK	–	–
1- or 2-Port Fast Ethernet, with 2-Slot WAN[3]	NM-1FE2W-V2 NM-2FE2W-V2	–	12.2(13)T	–
Wireless Multipoint Subscriber Unit	NM-WMDA	12.1(3)XQ1	–	–
Alarm Interface Card	NM-AIC-64	12.2(2)XG	–	–
16-Port Ethernet Switch	NM-ESW-161	12.2(2)XT	–	–
High-Density Analog Telephony	NM-HDA	12.2(2)XT	–	–
Content Engine for Caching and Content Delivery	NM-CE-BP	12.2(11)YT	12.2(13)T	–
Intrusion Detection System[2]	NM-CIDS-K9	12.2(15)ZJ1	–	–
1-Port T3/E3[4]	NM-1T3/E3	12.2(11)YT	12.2(15)T	–
1-Port Gigabit Ethernet[3]	NM-1GE	12.2(11)YT	12.2(15)T	–

1. Supported only by Cisco 2600XM routers.

2. Supported only by Cisco 2600XM and Cisco 2691 routers.
3. Supported only by Cisco 2691 routers.
4. Supported only by Cisco 2650 XM, Cisco 2651 XM, and Cisco 2691 routers.

Cisco 2600 Series 2-Slot Network Module Hardware Compatibility

Some network modules have two small slots, labeled W0 and W1, for WAN interface cards. Cisco 2600 series routers can use the zero-LAN 2-slot network module (NM-2W) only. This module is compatible with the following WAN interface cards:

- WIC-1T
- WIC-2T
- WIC-1B-S/T
- WIC-1B-U
- WIC-1DSU-56K
- WIC-1DSU-T1
- WIC-2A/S

For voice interface card support information, see Table 1-2.

Table 1-2 Voice Interface Card Support for Network Modules

Voice Interface Card	NM-1V	NM-2V	NM-HD-1V	NM-HD-2V	NM-HD-2VE	NM-HDV
VIC-2FXS	Yes	Yes	No	No	No	No
VIC-4FXS/DID	No	No	FXS only	FXS only	FXS only	No
VIC-2FXO	Yes	Yes	No	No	No	No
VIC-2FXO-M1	Yes	Yes	No	No	No	No
VIC-2FXO-EU	Yes	Yes	No	No	No	No
VIC-2FXO-M2	Yes	Yes	No	No	No	No
VIC-2FXO-M3	Yes	Yes	No	No	No	No
VIC-2E/M	Yes	Yes	No	No	No	No

Table 1-2 Voice Interface Card Support for Network Modules (continued)

Voice Interface Card	NM-1V	NM-2V	NM-HD-1V	NM-HD-2V	NM-HD-2VE	NM-HDV
VIC-2BRI-S/T-TE	Yes	Yes	No	No	No	No
VIC-2BRI-NT-TE	Yes	Yes	No	No	No	No
VIC-2DID	Yes	Yes	Yes	Yes	Yes	No
VIC-2CAMA	Yes	Yes	No	No	No	No
VWIC-1MFT-E1	No	No	No	No	Yes	Yes
VWIC-1MFT-T1	No	No	No	No	Yes	Yes
VWIC-2MFT-E1	No	No	No	No	Yes	Yes
VWIC-2MFT-T1	No	No	No	No	Yes	Yes
VWIC-2MFT-E1-DI	No	No	No	No	Yes	Yes
VWIC-2MFT-T1-DI	No	No	No	No	Yes	Yes
VIC2-2FXS	No	No	Yes	Yes	Yes	No
VIC2-2FXO	No	No	Yes	Yes	Yes	No
VIC2-4FXO	No	No	Yes	Yes	Yes	No
VIC2-2E/M	No	No	Yes	Yes	Yes	No
VIC2-2BRI-NT/TE	No	No	Yes	Yes	Yes	No
VWIC-2MFT-G.703	No	No	No	No	Yes	No

For more information about these WAN and voice interface cards, refer to the *Cisco Interface Cards Installation Guide*. To obtain this publication, see the "Obtaining Documentation" section on page xxvii.

Cisco 2600 Series Interface Numbering

Each network interface on a Cisco 2600 series router is identified by a slot number and a port number.

Slot and Port Numbering

The Cisco 2600 series router chassis contains one slot in which you can install a network module. This slot is always numbered 1. Both WAN interface card slots built into the chassis, W0 and W1, are always numbered slot 0.

Port numbers identify the interfaces on the modules and WAN interface cards installed in the router. Port numbers begin at 0 for each slot, and continue from right to left and (if necessary) from bottom to top. Modules and WAN interface cards are identified by interface type, slot number, a forward slash (/), and the port number, for example Ethernet 0/0.

Figure 1-1 shows a router with a 2E 2-slot module in slot 1. Two serial WAN interface cards are installed in the module.

Figure 1-1 Cisco 2600 and 2600XM Series Port Numbers

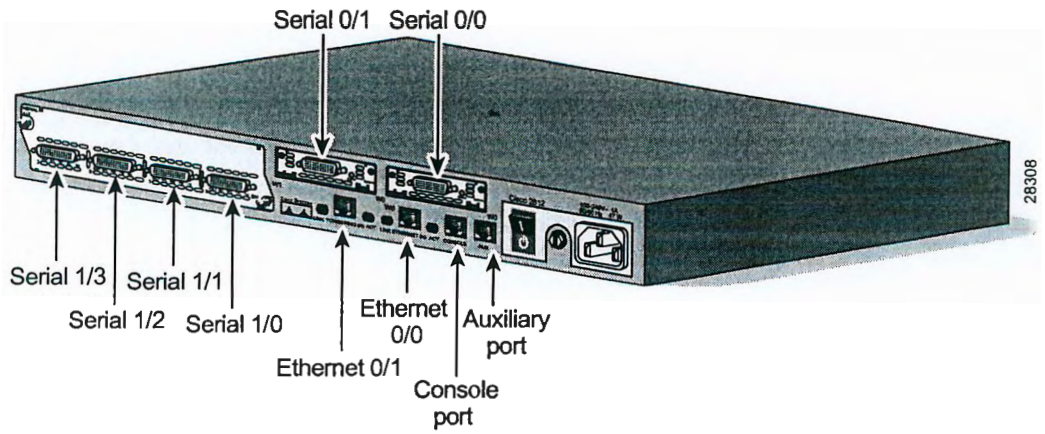


Figure 1-1 shows the following interface numbers:

- First Ethernet interface—Ethernet 0/0

Note Cisco 2600XM series routers substitute Fast Ethernet interfaces for the Ethernet interfaces used in Cisco 2600 series routers. For more information about interfaces available on your chassis, refer to the *Cisco 2600 Series Hardware Installation Guide*.

- Token Ring interface—Token Ring 0/0
- Slot W0, serial interface 0—Serial 0/0
- Slot W1, serial interface 1—Serial 0/1
- Slot 1, asynchronous/synchronous serial port 0—Serial 1/0
- Slot 1, asynchronous/synchronous serial port 1—Serial 1/1
- Slot 1, asynchronous/synchronous serial port 2—Serial 1/2
- Slot 1, asynchronous/synchronous serial port 3—Serial 1/3

Voice Interface Numbering in Cisco 2600 Series Routers

Voice interfaces are numbered differently from WAN interfaces. Voice interfaces are numbered as follows:

interface-type chassis-slot/voice module slot/voice port

If you have a four-channel voice network module installed in slot 1 of your router, the voice interfaces are:

- Slot 1, voice network module slot 0, voice port 0—Voice 1/0/0 (closest to the chassis WAN interface card slots)
- Slot 1, voice network module slot 0, voice port 1—Voice 1/0/1
- Slot 1, voice network module slot 1, voice port 0—Voice 1/1/0
- Slot 1, voice network module slot 1, voice port 1—Voice 1/1/1 (farthest from the chassis WAN interface card slots)

Cisco 3600 Series Routers

The Cisco 3600 series includes the Cisco 3620 router (see Figure 1-2), the Cisco 3640 and 3640A routers (see Figure 1-3), and the Cisco 3660 router (see Figure 1-4).

Note References to the Cisco 3660 router include the Cisco 3661 and Cisco 3662 models.

The Cisco 3620 has two network module slots, the Cisco 3640 has four slots, and the Cisco 3660 has six slots. Each network module slot accepts a variety of network module interface cards, supporting a variety of LAN and WAN technologies.

Figure 1-2 Cisco 3620 Router Rear View

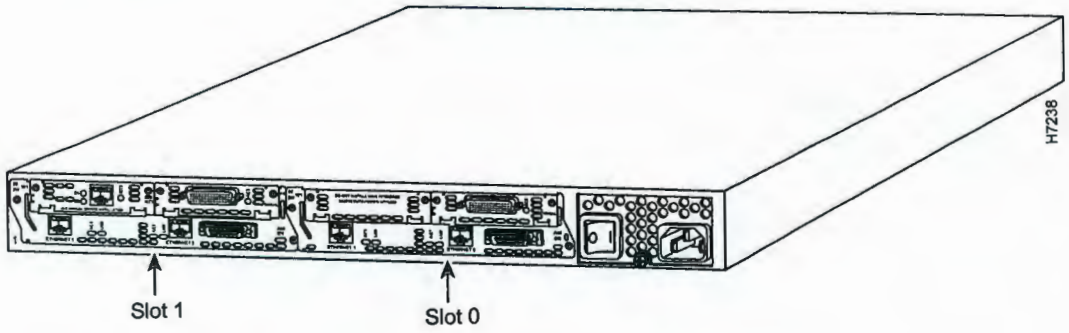


Figure 1-3 Cisco 3640 Router Rear View

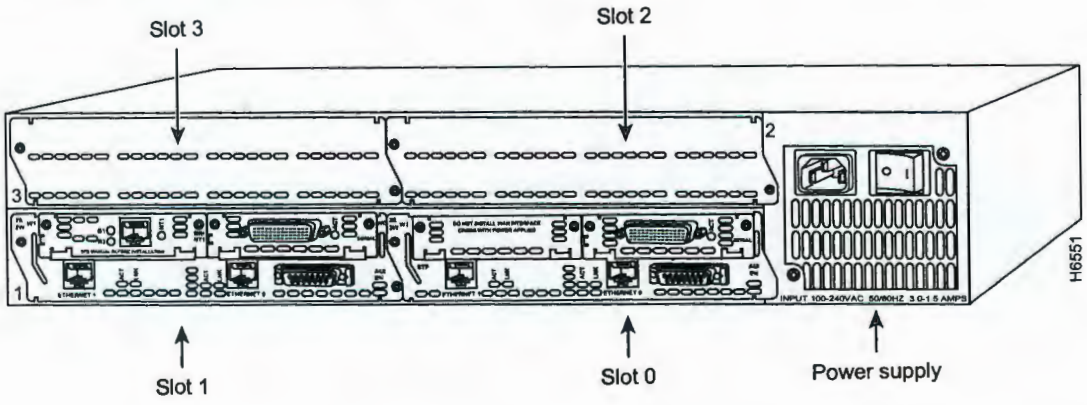


Figure 1-4 Cisco 3660 Router Rear View

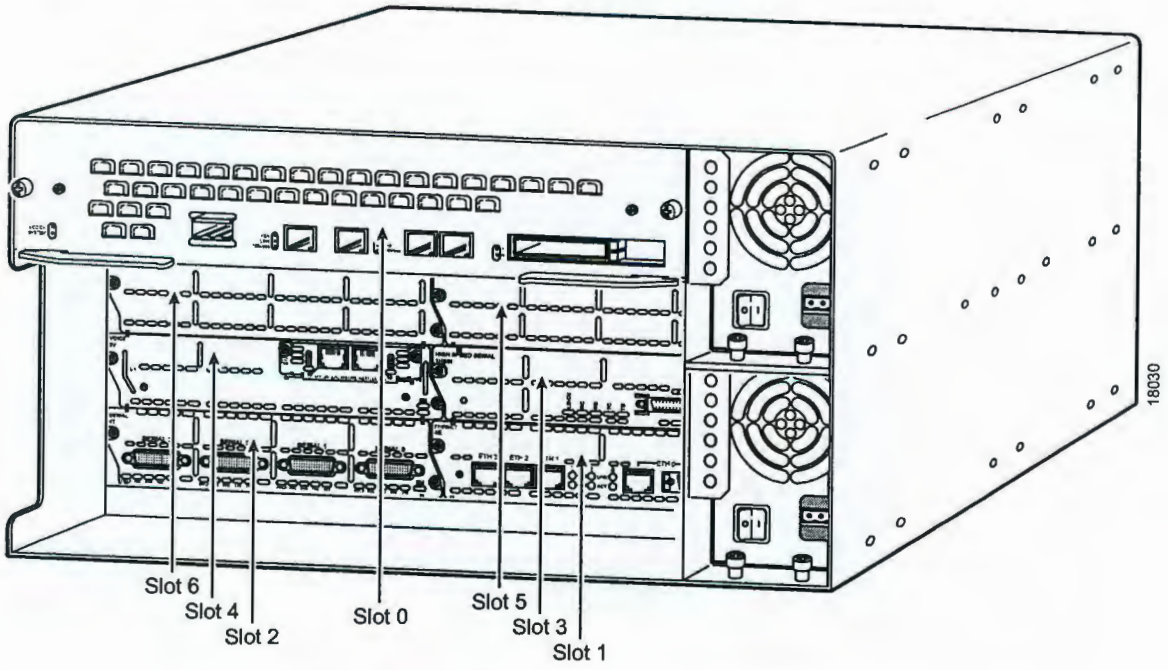


Table 1-3 lists network module options for Cisco 3600 series routers.

Table 1-3 Network Module Options for Cisco 3600 Series Routers

Network Module		Supported in Cisco IOS Releases:		
Description	Product Number	Specific Limited Lifetime	First "T" (Technology)	First Mainline
1-Port Ethernet	NM-1E	11.2(4)XA 11.2(5)P	11.3(1)T	11.3(1)
1-Port Fast Ethernet TX	NM-1FE-TX	11.2(6)P	11.3(1)T	11.3(1)
1-Port Fast Ethernet FX	NM-1FE-FX	–	11.3(1)T	–
1-Port Fast Ethernet, with 1- or 2-Port T1/ISDN PRI, with or without CSU	NM-1FE1CT1 NM-1FE1CT1-CSU NM-1FE2CT1 NM-1FE2CT1-CSU	12.0(7)XK	11.3(4)T1	–

Table 1-3 Network Module Options for Cisco 3600 Series Routers (continued)

Network Module		Supported in Cisco IOS Releases:		
Description	Product Number	Specific Limited Lifetime	First "T" (Technology)	First Mainline
1-Port Fast Ethernet, with 1- or 2-Port E1/ISDN PRI, Balanced or Unbalanced	NM-1FE1CE1B NM-1FE1CE1U NM-1FE2CE1B NM-1FE2CE1U	12.0(7)XK	11.3(4)T1	–
4-Port Ethernet	NM-4E	11.2(6)P	11.3(1)T	11.3(1)
1-Port Ethernet, with 2-Slot WAN	NM-1E2W	11.1(7)AA 11.2(4)XA 11.2(5)P	11.3(1)T	11.3(1)
2-Port Ethernet, with 2-Slot WAN	NM-2E2W	11.1(7)AA 11.2(4)XA 11.2(5)P	11.3(1)T	11.3(1)
1-Port Ethernet, with 1-Port Token Ring and 2-Slot WAN	NM-1E1R2W	11.1(8)AA 11.2(4)XA 11.2(5)XP	11.3(1)T	11.3(1)
4-Port Serial	NM-4T	11.2(4)XA 11.2(5)P	11.3(1)T	11.3(1)
4- or 8-Port Asynchronous/Synchronous Serial	NM-4A/S NM-8A/S	11.1(7)AA 11.2(4)XA 11.2(5)P	11.3(1)T	11.3(1)
16- or 32-Port Asynchronous Serial	NM-16A NM-32A	11.2(7a)P	11.3(1)T	11.3(1)
High-Density Voice	NM-HDV	–	12.0(6)T	–
4- or 8-Port ISDN BRI with S/T interface	NM-4B-S/T NM-8B-S/T	11.1(7)AA 11.2(4)XA 11.2(5)P 12.0(7)XK	11.3(1)T	11.3(1)
4- or 8-Port ISDN BRI with NT1 (U) interface	NM-4B-U NM-8B-U	11.1(7)AA 11.2(4)XA 11.2(5)P 12.0(7)XK	11.3(1)T	11.3(1)

Table 1-3 Network Module Options for Cisco 3600 Series Routers (continued)

Network Module		Supported in Cisco IOS Releases:		
Description	**Product Number**	**Specific Limited Lifetime**	**First "T" (Technology)**	**First Mainline**
1- or 2-Port Channelized T1/ISDN PRI	NM-1CT1 NM-2CT1	11.1(7)AA 11.2(4)XA 11.2(5)P 12.0(7)XK	11.3(1)T	11.3(1)
1- or 2-Port Channelized T1/ISDN PRI with CSU	NM-1CT1-CSU NM-2CT1-CSU	11.1(7)AA 11.2(4)XA 11.2(5)P 12.0(7)XK	11.3(1)T	11.3(1)
1- or 2-Port Channelized E1/ISDN PRI Unbalanced	NM-1CE1U NM-2CEIU	11.1(7)AA 11.2(4)XA 11.2(5)P 12.0(7)XK	11.3(1)T	11.3(1)
1- or 2-Port Channelized E1/ISDN PRI Balanced	NM-1CE1B NM-2CE1B	11.1(7)AA 11.2(4)XA 11.2(5)P 12.0(7)XK	11.3(1)T	11.3(1)
1- or 2-Port T1/E1 Channelized PRI with G.703[1]	NM-1CE1T1-PRI NM-2CE1T1-PRI	–	12.3T	–
1- or 2-Slot Voice	NM-1V NM-2V	–	11.3(1)T	–
1- or 2-Slot Voice[2]	NM-HD-1V NM-HD-2V NM-HD-2VE	12.2(15)ZJ	–	–
6-, 12-, 18-, 24-, or 30-Port Digital Modem[3]	NM-6DM NM-12DM NM-18DM NM-24DM NM-30DM	11.2(9)XA 11.2(10)P 12.0(7)XK	11.3(2)T	–
8- or 16-Port Analog Modem[4]	NM-8AM NM-16AM	12.0(7)XK	11.3(4)T	–
1-Port ATM-25	NM-1ATM-25	12.0(7)XK	11.3(3a)T	–

Table 1-3 Network Module Options for Cisco 3600 Series Routers (continued)

Network Module		Supported in Cisco IOS Releases:		
Description	**Product Number**	**Specific Limited Lifetime**	**First "T" (Technology)**	**First Mainline**
1-Port ATM T3/E3	NM-1A-T3 NM-1A-E3	–	12.1(2)T	–
1-Port ATM OC-3[5] (multimode, single-mode intermediate-reach, single-mode long-reach)	NM-1A-OC3MM NM-1A-OC3SMI NM-1A-OC3SML	–	12.0(3)T	–
1-Port ATM OC-3 Enhanced Performance (multimode, single-mode intermediate-reach, single-mode long-reach)	NM-1A-OC3MM-EP NM-1A-OC3-SMI-EP NM-1A-OC3SML-EP	–	12.2(13)T	–
1-Port OC-3/STM-1 ATM[5] Circuit Emulation Service (multimode, single-mode intermediate-reach, single-mode long-reach) with 1-Slot Voice	NM-1A-OC3MM-1V NM-1A-OC3SMI-1V NM-1A-OC3SML-1V	–	12.1(2)T	–
4- or 8-Port T1/E1 IMA	NM-8T1-IMA NM-4T1-IMA NM-8E1-IMA NM-4E1-IMA	–	12.0(5)T	–
0-, 1-, or 2-Port Fast Ethernet, with 2-WAN Card Slots	NM-2W NM-1FE2W NM-2FE2W	12.0(7)XK	12.1(1)T	–
1-Port Fast Ethernet, with 1-Port Token Ring and 2-Slot WAN	NM-1FE1R2W	12.0(7)XK	12.1(1)T	–
1- or 2-Port Fast Ethernet, with 2-Slot WAN	NM-1FE2W-V2 NM-2FE2W-V2	–	12.2(13)T	–

Table 1-3 Network Module Options for Cisco 3600 Series Routers (continued)

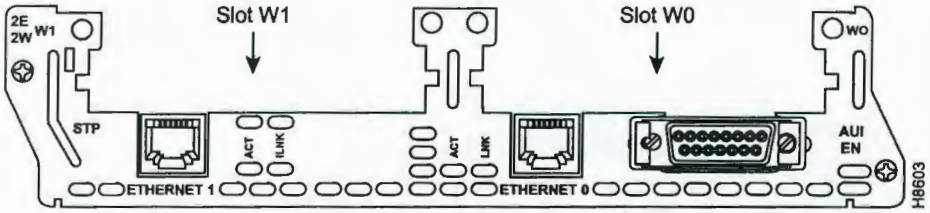
Network Module		Supported in Cisco IOS Releases:		
Description	**Product Number**	**Specific Limited Lifetime**	**First "T" (Technology)**	**First Mainline**
1-Port Fast Ethernet, with 1-Port Token Ring and 2-Slot WAN	NM-1FE1R2W-V2	–		–
1-Port HSSI	NM-1HSSI	–	11.3(3)T	–
Compression	NM-COMPR	–	11.3(1)T	–
Wireless Multipoint Subscriber Unit	NM-WMDA	12.1(3)XQ1	–	–
Alarm Interface Card	NM-AIC-64	12.2(2)XG	–	–
16-Port Ethernet Switch	NM-ESW-161	12.2(2)XT	–	–
High-Density Analog Telephony	NM-HDA	12.2(2)XT	–	–
Content Engine for Caching and Content Delivery[6]	NM-CE-BP	12.2(11)YT	12.2(13)T	–
Intrusion Detection System[7]	NM-CIDS-K9	12.2(15)ZJ1	–	–
1-Port T3/E3[7]	NM-1T3/E3	12.2(11)YT	12.2(15)T	–
1-Port Gigabit Ethernet[7]	NM-1GE	12.2(11)YT	12.2(15)T	–

1. Supported only by Cisco 3631 and Cisco 3660 routers.
2. Supported only by Cisco 3640 and Cisco 3660 routers.
3. Digital modem network modules do not have online insertion and removal (OIR) functionality implemented in this Cisco IOS release.
4. Analog modem network modules do not have OIR functionality implemented in this Cisco IOS release.
5. Not supported by Cisco 3631 routers.
6. Not supported by Cisco 362*x* routers.
7. Supported only by Cisco 3660 routers.

Cisco 3600 Series 2-Slot Network Module Hardware Compatibility

Some network modules have two small slots, labeled W0 and W1, for WAN interface cards. Figure 1-5 shows the W0 and W1 slots of the 2-Ethernet 2-WAN card slot module.

Figure 1-5 WAN Interface Card Slots



All 2-slot network modules are compatible with the following WAN interface cards:

- WIC-1T
- WIC-2T
- WIC-1B-S/T
- WIC-1B-U
- WIC-1DSU-56K
- WIC-1DSU-T1
- WIC-2A/S

For voice interface card support information, see Table 1-4.

Table 1-4 Voice Interface Card Support for Network Modules

Voice Interface Card	NM-1V	NM-2V	NM-HD-1V	NM-HD-2V	NM-HD-2VE	NM-HDV
VIC-2FXS	Yes	Yes	No	No	No	No
VIC-4FXS/DID	No	No	FXS only	FXS only	FXS only	No
VIC-2FXO	Yes	Yes	No	No	No	No

Table 1-4 Voice Interface Card Support for Network Modules (continued)

Voice Interface Card	NM-1V	NM-2V	NM-HD-1V	NM-HD-2V	NM-HD-2VE	NM-HDV
VIC-2FXO-M1	Yes	Yes	No	No	No	No
VIC-2FXO-EU	Yes	Yes	No	No	No	No
VIC-2FXO-M2	Yes	Yes	No	No	No	No
VIC-2FXO-M3	Yes	Yes	No	No	No	No
VIC-2E/M	Yes	Yes	No	No	No	No
VIC-2BRI-S/T-TE	Yes	Yes	No	No	No	No
VIC-2BRI-NT-TE	Yes	Yes	No	No	No	No
VIC-2DID	Yes	Yes	Yes	Yes	Yes	No
VIC-2CAMA	Yes	Yes	No	No	No	No
VWIC-1MFT-E1	No	No	No	No	Yes	Yes
VWIC-1MFT-T1	No	No	No	No	Yes	Yes
VWIC-2MFT-E1	No	No	No	No	Yes	Yes
VWIC-2MFT-T1	No	No	No	No	Yes	Yes
VWIC-2MFT-E1-DI	No	No	No	No	Yes	Yes
VWIC-2MFT-T1-DI	No	No	No	No	Yes	Yes
VIC2-2FXS	No	No	Yes	Yes	Yes	No
VIC2-2FXO	No	No	Yes	Yes	Yes	No
VIC2-4FXO	No	No	Yes	Yes	Yes	No
VIC2-2E/M	No	No	Yes	Yes	Yes	No
VIC2-2BRI-NT/TE	No	No	Yes	Yes	Yes	No
VWIC-2MFT-G.703	No	No	No	No	Yes	No

For more information about these WAN interface cards, refer to the *WAN Interface Cards Hardware Installation Guide*. To obtain this publication, see the "Obtaining Documentation" section on page xxvii.

Cisco 3600 Series Interface Numbering

Each network interface on a Cisco 3600 series router is identified by a slot number and a port number.

Slot Numbering

A Cisco 3600 series router chassis contains two, four, or six slots in which you can install modules. You can install any module into any available slot in the chassis.

For the Cisco 3620 router, shown in Figure 1-2, the slots are numbered as follows:

- Slot 0 is at the bottom right (as viewed from the rear of the chassis), near the power supply.
- Slot 1 is at the bottom left.

The Cisco 3640 router, shown in Figure 1-3, has the following additional slots:

- Slot 2 is at the top right, above slot 0.
- Slot 3 is at the top left, above slot 1.

The Cisco 3660 router, shown in Figure 1-4, uses a different numbering system:

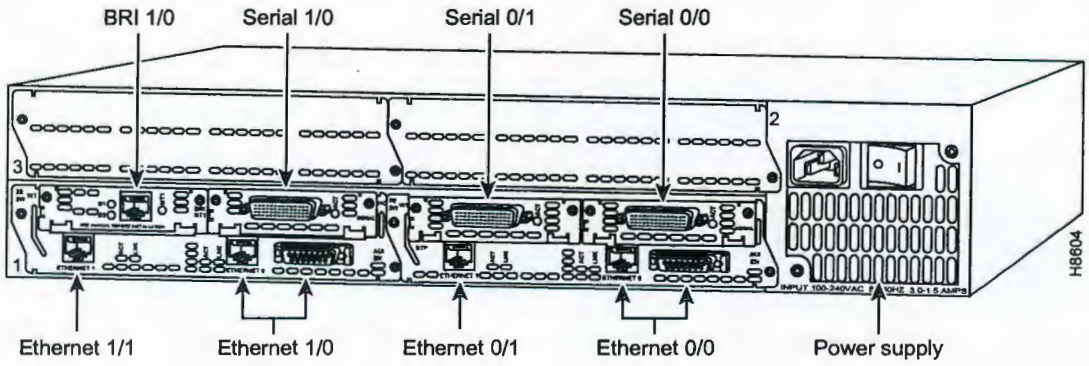
- Slot 0 contains fixed Fast Ethernet ports and is located at the top of the chassis.
- Slot 1 is at the bottom right (as viewed from the rear of the chassis), near the power supply.
- Slot 2 is at the bottom left.
- Slot 3 is at the right, above slot 1.
- Slot 4 is at the left, above slot 2.
- Slot 5 is at the right, above slot 3.
- Slot 6 is at the left, above slot 4.

Port Numbering

Port numbers begin at 0 for each slot, and continue from right to left and (if necessary) from bottom to top. Modules and WAN interface cards are identified by interface type, slot number, a forward slash (/), and the port number, for example Ethernet 0/0.

Figure 1-6 shows a router with 2-Ethernet 2-slot modules in slot 0 and slot 1. Two serial WAN interface cards are installed in the module in slot 0. One serial and one ISDN BRI WAN interface card are installed in the module in slot 1.

Figure 1-6 Cisco 3600 Series Port Numbers



As shown in Figure 1-6, the port numbers for this router are:

- Slot 0, Ethernet interface 0—Ethernet 0/0
- Slot 0, Ethernet interface 1—Ethernet 0/1
- Slot 0, serial interface 0—Serial 0/0
- Slot 0, serial interface 1—Serial 0/1
- Slot 1, Ethernet interface 0—Ethernet 1/0

- Slot 1, Ethernet interface 1—Ethernet 1/1
- Slot 1, serial interface 0—Serial 1/0
- Slot 1, BRI interface 0—BRI 1/0

Note The 2-Ethernet 2-slot module described in this example provides both an attachment unit interface (AUI) and a 10BASE-T connector for port 0. Only one of these connectors can be used at a time.

Voice Interface Numbering in Cisco 3600 Series Routers

Voice interfaces are numbered differently from WAN interfaces. Voice interfaces are numbered as follows:

interface-type chassis-slot/voice module slot/voice port

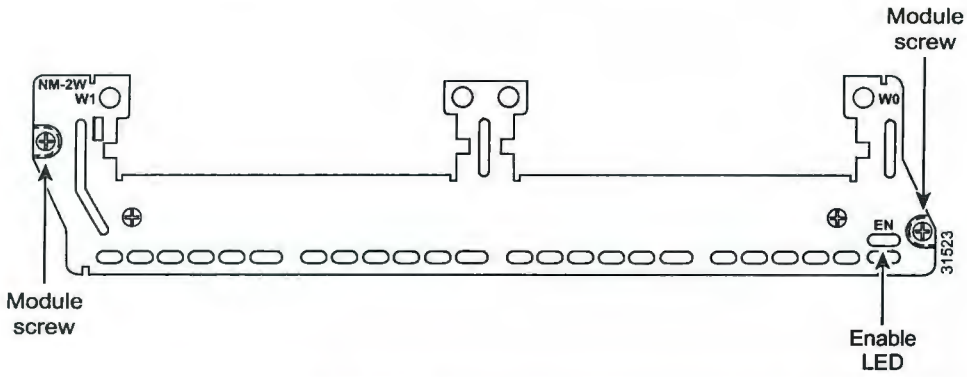
If you have a 4-channel voice network module installed in slot 1 of your router, the voice interfaces are:

- Slot 1, voice network module slot 0, voice port 0—Voice 1/0/0 (closest to chassis slot 0)
- Slot 1, voice network module slot 0, voice port 1—Voice 1/0/1
- Slot 1, voice network module slot 1, voice port 0—Voice 1/1/0
- Slot 1, voice network module slot 1, voice port 1—Voice 1/1/1 (farthest from chassis slot 0)

2-WAN Interface Card Network Module

The 2-WAN interface card (WIC) network module, Cisco part number NM-2W, provides two slots for optional WAN interface cards (see Figure 1-7). These modules have no network connectors. WAN interface cards installed in the network module provide the connection to the network. WAN interface cards are described in the *Cisco Interface Cards Installation Guide*.

Figure 1-7 2-WIC Network Module



The 2-WAN interface card network module has an enable (EN) LED. This LED indicates that the module has passed its self-tests and is available to the router (see Figure 1-7).

Cisco 3700 Series Routers

The Cisco 3700 series includes the Cisco 3725 router and the Cisco 3745 router. The Cisco 3725 has two network module slots, one of which can accommodate a double-width network module. The Cisco 3745 has four slots and can accommodate up to two double-width network modules. Figure 1-8 shows Cisco 3725 slot numbers. Figure 1-9 show slot numbering for the Cisco 3745 with both single- and double-width network modules installed.

Figure 1-8 Cisco 3725 Router Rear View

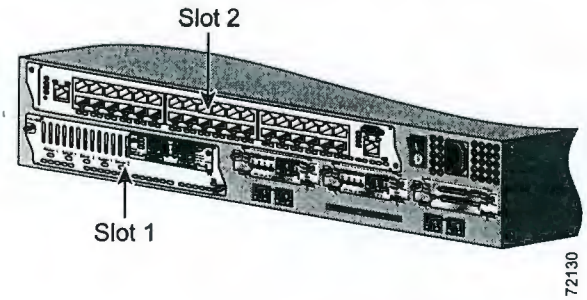


Figure 1-9 Cisco 3745 Router Rear View

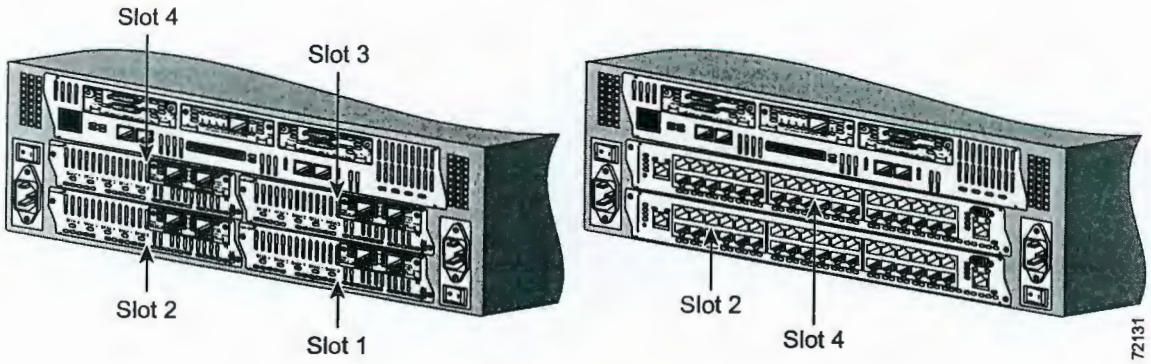


Table 1-5 lists network module options for Cisco 3700 series routers, with minimum software requirements for Cisco IOS Releases 12.2T.

Table 1-5 Network Modules Options for Cisco 3700 Series Routers

Network Module		Supported in Cisco IOS Release		
Description	Product Number	Specific Limited Lifetime	First "T" (Technology)	First Mainline
16-Port Ethernet Switch	NM-ESW-16	–	12.2(8)T	–
1-Port ATM T3/E3	NM-1A-T3 NM-1A-E3	–	12.2(8)T	–
1-Port Fast Ethernet, with 1-Port Token Ring and 2-Slot WAN	NM-1FE1R2W	–	12.2(8)T	–
1-Port HSSI	NM-1HSSI	–	12.2(8)T	–
1- or 2-Port Channelized E1/ISDN PRI Balanced	NM-1CE1B NM-2CE1B	–	12.2(8)T	–
1- or 2-Port Channelized E1/ISDN PRI Unbalanced	NM-1CE1U NM-2CE1U	–	12.2(8)T	–
1- or 2-Port Channelized T1/ISDN PRI with CSU	NM-1CT1-CSU NM-2CT1-CSU	–	12.2(8)T	

Table 1-5 Network Modules Options for Cisco 3700 Series Routers (continued)

Network Module		Supported in Cisco IOS Release		
Description	Product Number	Specific Limited Lifetime	First "T" (Technology)	First Mainline
1- or 2-Port Channelized T1/ISDN PRI	NM-1CT1 NM-2CT1	–	12.2(8)T	–
1- or 2-Port T1/E1 Channelized PRI with G.703	NM-1CE1T1-PRI NM-2CE1T1-PRI	–	12.3T	–
0-, 1-, or 2-Port Fast Ethernet, with 2-Slot WAN	NM-2W NM-1FE2W NM-2FE2W	–	12.2(8)T	–
1- or 2-Port Fast Ethernet, with 2-Slot WAN	NM-1FE2W-V2 NM-2FE2W-V2	–	12.2(13)T	–
1-Port Fast Ethernet, with 1-Port Token Ring and 2-Slot WAN	NM-1FE1R2W-V2	–		–
1- or 2-Slot Voice	NM-1V NM-2V	–	12.2(8)T	–
1- or 2-Slot Voice	NM-HD-1V NM-HD-2V NM-HD-2VE	12.2(15)ZJ	–	–
6-, 12-, 18-, 24-, or 30-Port Digital Modem	NM-6DM NM-12DM NM-18DM NM-24DM NM-30DM	–	12.2(8)T	–
4- or 8-Port Asynchronous/Synchronous Serial	NM-4A/S NM-8A/S	–	12.2(8)T	–
4- or 8-Port ISDN BRI with S/T Interface	NM-4B-S/T NM-8B-S/T	–	12.2(8)T	–
4- or 8-Port ISDN BRI with NT1 (U) Interface	NM-4B-U NM-8B-U	–	12.2(8)T	–

Table 1-5 Network Modules Options for Cisco 3700 Series Routers (continued)

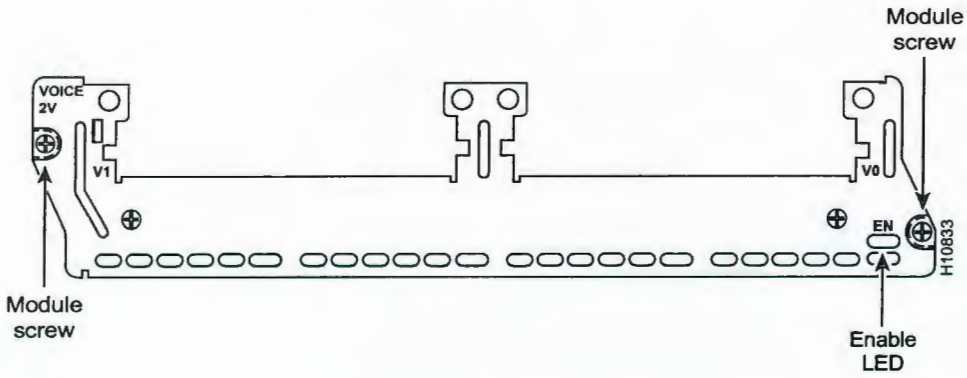
Network Module		Supported in Cisco IOS Release		
Description	Product Number	Specific Limited Lifetime	First "T" (Technology)	First Mainline
4- or 8-Port T1/E1 IMA	NM-8E1-IMA NM-4E1-IMA NM-4T1-IMA NM-8T1-IMA	–	12.2(8)T	–
High-Density Voice	NM-HDV	–	12.2(8)T	–
High-Density Analog Voice	NM-HDA	–	12.2(8)T	–
1-Port Fast Ethernet FX	NM-1FE-FX	12.2(11)YT	12.2(13)T	–
1-Port OC-3/STM-1 ATM[5] Circuit Emulation Service (multimode, single-mode intermediate-reach, single-mode long-reach) with 1-Slot Voice	NM-1A-OC3MM-1V NM-1A-OC3SMI-1V NM-1A-OC3SML-1V	12.2(11)YT	12.12(13)T	–
1-Port ATM OC-3 Enhanced Performance (multimode, single-mode intermediate-reach, single-mode long-reach)	NM-1A-OC3MM-EP NM-1A-OC3-SMI-EP NM-1A-OC3SML-EP	–	12.2(13)T	–
16- or 32-Port Asynchronous Serial[1]	NM-16A NM-32A	12.2(11)YT	12.2(13)T	–
8- or 16-Port Analog Modem[2]	NM-8AM NM-16AM	12.2(11)YT	12.2(13)T	–
Content Engine for Caching and Content Delivery	NM-CE-BP	12.2(11)YT	12.2(13)T	–
Intrusion Detection System	NM-CIDS-K9	12.2(15)ZJ1	–	–
1-Port T3/E3	NM-1T3/E3	12.2(11)YT	12.2(15)T	–
1-Port Gigabit Ethernet	NM-1GE	12.2(11)YT	12.2(15)T	–

1. Not supported on Cisco 3725 routers.
2. Not supported on Cisco 3725 routers.

Voice Network Modules

Voice interface cards cannot be installed in a built-in interface card slot on a Cisco 3700 series router. Instead they must be installed in a voice network module, such as the one shown in Figure 1-10.

Figure 1-10 4-Channel Voice Network Module



For voice interface card support information, see Table 1-6.

Table 1-6 Voice Interface Card Support for Network Modules

Voice Interface Card	NM-1V	NM-2V	NM-HD-1V	NM-HD-2V	NM-HD-2VE	NM-HDV
VIC-2FXS	Yes	Yes	No	No	No	No
VIC-4FXS/DID	No	No	FXS only	FXS only	FXS only	No
VIC-2FXO	Yes	Yes	No	No	No	No
VIC-2FXO-M1	Yes	Yes	No	No	No	No
VIC-2FXO-EU	Yes	Yes	No	No	No	No
VIC-2FXO-M2	Yes	Yes	No	No	No	No
VIC-2FXO-M3	Yes	Yes	No	No	No	No
VIC-2E/M	Yes	Yes	No	No	No	No
VIC-2BRI-S/T-TE	Yes	Yes	No	No	No	No
VIC-2BRI-NT-TE	Yes	Yes	No	No	No	No

Table 1-6 Voice Interface Card Support for Network Modules (continued)

Voice Interface Card	NM-1V	NM-2V	NM-HD-1V	NM-HD-2V	NM-HD-2VE	NM-HDV
VIC-2DID	Yes	Yes	Yes	Yes	Yes	No
VIC-2CAMA	Yes	Yes	No	No	No	No
VWIC-1MFT-E1	No	No	No	No	Yes	Yes
VWIC-1MFT-T1	No	No	No	No	Yes	Yes
VWIC-2MFT-E1	No	No	No	No	Yes	Yes
VWIC-2MFT-T1	No	No	No	No	Yes	Yes
VWIC-2MFT-E1-DI	No	No	No	No	Yes	Yes
VWIC-2MFT-T1-DI	No	No	No	No	Yes	Yes
VIC2-2FXS	No	No	Yes	Yes	Yes	No
VIC2-2FXO	No	No	Yes	Yes	Yes	No
VIC2-4FXO	No	No	Yes	Yes	Yes	No
VIC2-2E/M	No	No	Yes	Yes	Yes	No
VIC2-2BRI-NT/TE	No	No	Yes	Yes	Yes	No
VWIC-2MFT-G.703	No	No	No	No	Yes	No

For more information on using voice network modules, refer to Chapter 9, "Connecting Voice Network Modules."

All 2-slot network modules are compatible with the following WAN interface cards:

- WIC-1T
- WIC-2T
- WIC-1B-S/T
- WIC-1B-U
- WIC-1DSU-56K
- WIC-1DSU-T1
- WIC-2A/S

Cisco 3700 Series Interface Numbering

Each network interface on a Cisco 3700 series router is identified by a slot number and a port number.

Slot Numbering

A Cisco 3725 router includes two slots in which you can install network modules. The upper slots can be accommodate either a single- or a double-width network module. The slot numbers are as follows:

- 1 for interfaces in the lower network module slot
- 2 for interfaces in the upper-right network module slot (single- or double-width)

A Cisco 3745 router includes four slots in which you can install network modules. Each pair of slots can be combined to accommodate a double-width network module. The slot numbers are as follows:

- 1 for interfaces in the lower-right network module slot
- 2 for interfaces in the lower-left network module slot
- 3 for interfaces in the upper-right network module slot
- 4 for interfaces in the upper-left network module slot
- 2 for interfaces in the lower double-width slot
- 4 for interfaces in the upper double-width slot

Port Numbering

Port numbers begin at 0 for each slot, and continue from right to left and (if necessary) from bottom to top. Modules and WAN interface cards are identified by interface type, slot number, a forward slash (/), and the port number, for example, FastEthernet 0/0.

Figure 1-11 shows an example of interface numbering on a Cisco 3725 router with the following configuration:

- A WIC in each WIC slot
- A 2-port T1 network module in slot 1 (containing the following ports: T1 1/0 and T1 1/1)

DOC.
000233

CPL/AC

PREGÃO
050/2003

LOCAÇÃO DE EQUIPAMENTOS DE INFORMÁTICA INCLUINDO ASSISTÊNCIA TÉCNICA E TREINAMENTO

COBRA TECNOLOGIA – MANUAL VOLUME 13

2003
PASTA 41

ServerWorks
A BROADCOM Company

Products

Grand Champion HE

Features

Pentium 4® Xeon™ GC-HE SystemI/O™

- Host Bridge - CMIC-HE
- I/O Bridges - 0-3 CIOB-X
- South Bridge - CSB5, CSB6
- Memory/Address Buffers - 5-10 REMC

CMIC-HE

- Processor Interface
  - 4-Way Pentium 4® Xeon™
  - 400 MHz Front Side Bus
- Memory Controller
  - Four DDR200 channels
  - 64GB of memory
  - 6.4GB/s memory bandwidth
- I/O bridge interface
  - 3 Inter-Module Buses (IMB)
  - 1.6GB/s per bus
  - 1 Thin-IMB to the south bridge

RAS Features

- ECC - 128 bit algorithm
- 16bit detection; 8 bit correction
- Memory Scrubbing, Chipkill™
- Spare Memory
- Memory Mirroring
- Hot Plug Memory Card
- Extensive error reporting

CIOB-X

- Dual PCI-X Buses
- 64bit, 66/100 MHz

CSB6

- PCI 2.2 64-bit/33MHz
- Legacy functions (8237DMA, 8259PIC,

Summary of B

4-Way Pentiu

Performance, Availability, M

Industry leadi

- 4 Way M memory
- Bandwic
  - 5.
  - 3
  - 6.

Built in Scalab

- Up to 6
- Up to 6
- Configu

High Reliabilit

- Memory
  - In de al
  - Me
- Memory corrupti
  - Ch
  - Sp tra m
- Hot plug
  - Up sy
- PCI-X h

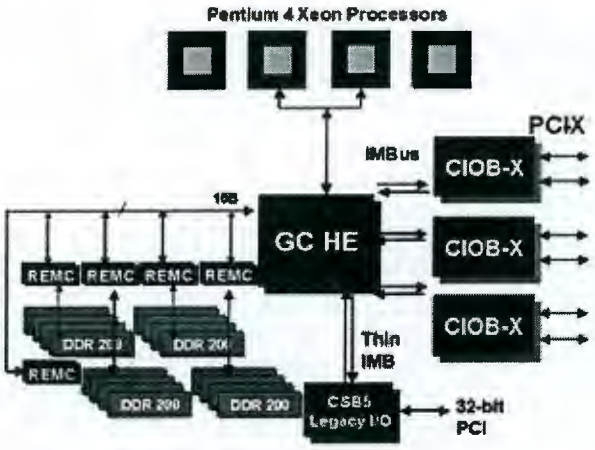
The GC-HE utili: host bridge to a bridges. This bu

146

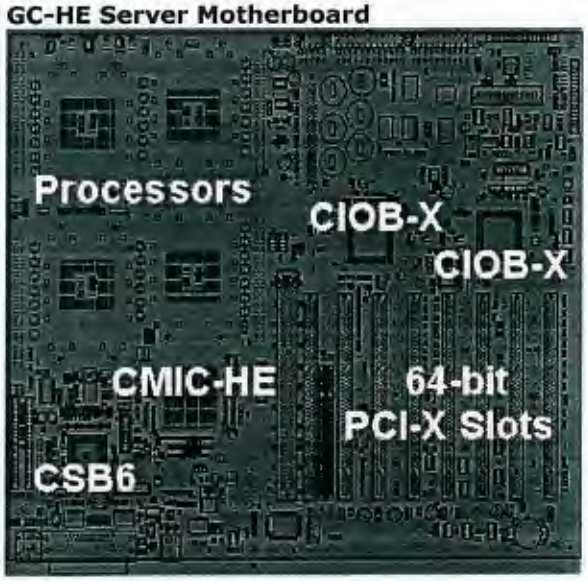
8254Timer)
- PCI to LPC bridge
- XIO-APIC for multiprocessor systems.
- 4 Port USB interface
- ACPI power management and event detection support
- Three ATA channels supporting up to 6 hard disk drives
- Server Appliance functions: Watchdog timer, NVRAM support, LCD and Keypad support

across all Serve
offers ease of p
reconfiguration

2 Way Multiprocessing Server Configuration



GC-HE Server Motherboard



Grand Champi

The Grand Char
Performance 4-
scaleable Syste
Xeon™ family o
configured to m
product segmer

The Grand Char
performance 2 :
solution on the
channels, capat
DDR200 memor
memory bandw
complement me
balanced archit
support for up t
with 4.8GB/s of
fold increase ov
The high bandw
interfaces provi
generation ente
memory and ad
interleaved mer

The GC-HE is ar
a RAS perspecti
memory scrubb
assured that yo
a failure does o
Memory configu
to the end user
allows IT manag
memory module
more reliability
memory card c
memory and m
features, like IM
PCI-X allow for
features can be
network level, t
BCM5700 or BC
to provide failo

Send to a Friend >

ServerWorks
A BROADCOM Company

PRODUCTS NEWS & EVENTS COMPANY TECHNOLOGY SUPPORT

Products

Grand Champion LE

Features

Pentium 4® Xeon™ GC-LE SystemI/O™

- Host Bridge - CMIC-LE
- I/O Bridge - CIOB-X2, CIOB-E
- South Bridge - CSB5, CSB6

CMIC-LE

- Processor Interface
  - 2-Way Pentium 4® Xeon™
  - 533MHz Front Side Bus
  - 4.2 GB/s FSB bandwidth
- Memory Controller
  - Dual DDR266 channels
  - 16GB of memory
  - 2 Way Interleaved
  - 4.1GB/s memory bandwidth
- I/O bridge interface
  - 2 Inter-Module Buses (IMB) 3.2GB/s per bus
  - 1 Thin-IMB to the south bridge

RAS Features

- ECC - 128 bit algorithm
- 8bit detection, 4 bit correction
- Memory Scrubbing, Chipkill™
- Spare Memory
- Fault isolation
- Extensive error reporting

CIOB-E

- Dual Gigabit Ethernet ports
- Integrated 66/100/133 MHz PCI-X

CIOB-X2

- Dual PCI-X Buses
- 64bit, 66/100/133MHz PCI-X

Summary of B

Volume 2-Wa

Performance, Availability, M

Industry leadi

- 2 Way M memory
- Bandwic
  - 6. IM in
  - 4. ba
  - 4.

Scales to mee

- Up to 4
- Up to 1€
- Configu

High Reliabilit

- Memory
  - 8t
  - Me
- Memory corrupti
  - Ch
  - Sp tra m co
- CRC che
- PCI-X h

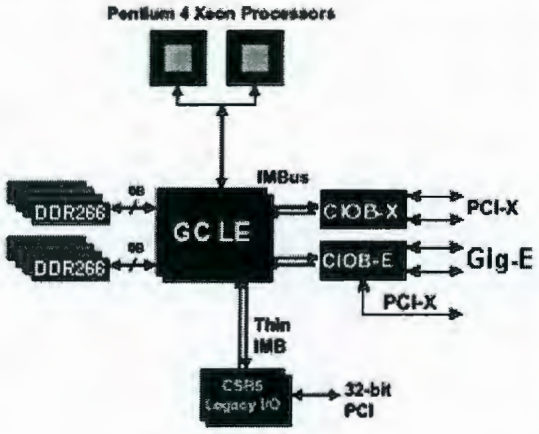
The GC-LE utiliz host bridge to a bridges. This bu

148

CSB6

- PCI 2.2 64-bit/33MHz
- Legacy functions (8237DMA, 8259PIC, 8254Timer)
- PCI to LPC bridge
- XIO-APIC for multiprocessor systems
- 4 Port USB interface
- ACPI power management and event detection support
- Three ATA channels supporting up to 6 hard disk drives
- Server Appliance functions: Watchdog timer, NVRAM support, LCD and Keypad support

2 Way Multiprocessing Server Configuration



GC-LE Server Motherboard

across all Serve
offers ease of p
reconfiguration

Grand Champi

The Grand Char
2-Way server m
SystemI/O™ so
Pentium 4® Xe
be configured t
of product segm

The Grand Char
performance 2-
solution on the
channels capabl
DDR266 memo
memory bandw
bandwidth com
well balanced a
provide support
buses, with 6.4
provides 4.1GB,
over the Pentiu
bandwidth, low
interfaces provi
generation ente
the integrated r
small form fact
and 2U rack ser

The GC-LE is ar
RAS perspective
algorithm, mem
can be assured
maintained. If a
supports Spare
failure will be in
managers can t
at their conveni
provided on the
protected, and
Extending the R
the GC-LE can b
BCM5701 Gigat
and load balanc

149

Send to a Friend > | Products | News & Events | Company | Technology | Support | Careers | Contact

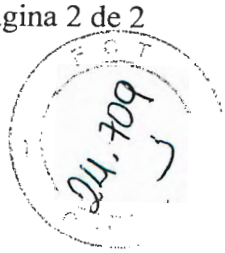
Sudhian Media

[redacted]

Compaq HP , 72.8 GB (286714-B22) Hard Drive: Product Features (choose a different model)

Compaq hard disk drives undergo an intense qualification process that eliminates data integrity problems, firmware and O/S incompatibilities, and other causes of data corruption or premature failure. Compaq hard disk drives are specifically designed and tested for flawless operation in your equipment. Supply your server, workstation or notebook with a Compaq hard disk drive and you will prevent incompatibilities that can rob your system of performance or cause you to lose valuable data.This HDD is designed for any Ultra 320, Ultra3 or Ultra2 capable ProLiant Servers, ProLiant Storage Systems, AlphaServers, and StorageWorks HP enclosures.

Key Features	
Storage Type	Hard drive
Type	Hot-Swap
Capacity	72.8 GB
Interface	SCSI Ultra320
Enclosure	Plug-In Module
Form Factor	3.5" x 1/3H
Spindle Speed	10000 rpm
Platform	PC
Technical Features	
Seek Time	4.9 ms
Data Transfer Rate	320 MBps
SCSI Signaling Typ	Low Voltage Differential (LVD)
Controller	
Controller Type	None
Other Features	
Package Qty.	1
Dimensions	
Height	.99 in.
Width	4.02 in.



Miscellaneous

DealTime Product ID 20303755

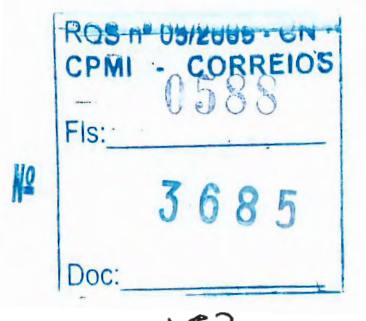
Compare Prices & Buy

Alternate Resources

Discount Compaq Solutions
Same day shipments, 286713-B22 memory, cpu, drives, servers & more
www.channe supporgroup.com

Hot Swap/Plug Specialists
Hot Plug Hot Swap Disk Drives for HP Proliant and Netservers
www.e4ServicesInc.com

Compaq Parts
For old and new Proliant Servers and storage contact us for any part
www.us21computers.com



152

QuickSpecs

Compaq NC7770 PCI-X Gigabit Server Adapter

Models

Compaq NC7770 PCI-X Gigabit Server Adapter

244948-B21

The Compaq NC7770 PCI-X Gigabit Server Adapter is the first in a new generation of networking solutions to combine Gigabit Ethernet speed with PCI-X bus technology. The NC7770 is a single port copper Gigabit server adapter that runs over Category 5 (or better) twisted-pair cabling. Along with all the advanced features that ProLiant customers have come to expect, the NC7770 includes support for Jumbo Frames, Wake on LAN (WOL), Dual Address Cycles (DAC), and Pre-Boot Execution environment (PXE).

Fast Ethernet Server Adapters:

NC3123 PCI, 10/100 WOL
174830-B21

NC3134: Fast Ethernet NIC 64 PCI Dual Base 10/100
138603-B21

PCI Gigabit Server Adapters and Upgrade Modules:

NC7131 Gigabit Server Adapter PCI, 64/66, 10/100/1000-T
158575-B21

NC6136 Gigabit Server Adapter PCI, 64/66, 1000-SX
203539-B21

NC6132 1000 SX Upgrade Module
338456-B23

NC6133 1000 LX Upgrade Module
338456-B24

NC7132 10/100/1000-T Upgrade Module
153543-B21

Overview

The NC7770 supports 10/100/1000Mbps Ethernet speeds as well as a PCI-X 64-bit/133MHz data path, backwards compatible with existing PCI bus architectures. This range of features enables Compaq customers to protect their current hardware investment while also future-proofing their ProLiant servers for the inevitable increase in networking throughput. Additionally, the NC7770 ships with support for PCI Hot Plug, Network Fault Tolerance, Load Balancing, Jumbo Frames, and various offload capabilities that improve performance. These improvements in speed and throughput come at a cost-effective price for environments using Category 5 (or better) twisted-pair cabling.

Performance

Gigabit Ethernet Throughput

Up to 1000Mbps Ethernet transfer rate delivers outstanding network performance that improves response time and removes bottlenecks across the entire network.

PCI-X Data Path

Compaq was an early champion of PCI-X bus technology and has played a key role in the development and industry adoption of the PCI-X specification. The NC7770 is Compaq's first server adapter to feature a PCI-X 64-bit/133MHz data path, which yields faster transmissions with lower CPU utilization.

153

Load Balancing

Transmit Load Balancing (TLB) and Switch-Assisted Load Balancing (SLB) are two advanced features used to build a bigger pipe for improved networking bandwidth. These port bonding techniques enable users to install up to eight NC7770 adapters in a ProLiant server and aggregate their throughput up to a maximum of 16Gigabits per second full-duplex transmissions.

Jumbo Frames

Jumbo Frames (also known as Extended Frames) offer a 9K byte Maximum Transmission Unit (MTU), which is six times the size of traditional Ethernet frames. Like all Compaq Gigabit server adapters, the NC7770 supports jumbo frames as a way to achieve higher throughput and better CPU utilization when deployed in a network infrastructure that supports them. Jumbo frames are particularly useful for database transfers and tape backups.

TCP Offloads and Interrupt Coalescing

The NC7770 features TCP Checksum Offloads as well as TCP Segmentation Offloads. Both reduce the load on the CPU for overall improved system response. Interrupt Coalescence is a feature that groups multiple packets and issues a single interrupt to the host. This process optimizes host efficiency, leaving the CPU available for other duties.

Scalability and Reliability

Tri-Speed Support

Because the NC7770 supports both 10Mbps Ethernet and 100Mbps Fast Ethernet in addition to Gigabit Ethernet, users are guaranteed end-to-end protocol support across their enterprise. Like all Compaq server adapters, the NC7770 adheres to open industry standards, insuring that it will work seamlessly with any network devices that also support IEEE standards.

PCI-X Support for Traditional PCI slots

PCI-X technology insures hardware investment protection by retaining backward compatibility with the standard PCI bus architecture at the device and driver level. When the NC7770 is used in a 64/100, 64/66, 64/33, or 32/33 IO slot, the performance is limited to the maximums of those conventional bus architectures.

Network Fault Tolerance (NFT)

Network Fault Tolerance, sometimes called "failover" or "NIC Redundancy," allows for the installation of multiple NC7770 server adapters so that the active device can be backed up by a redundant adapter to improve availability. Compaq's teaming utility also allows users to specify that when a failed adapter is fixed and replaced, the original adapter resumes its function as the primary network connection.

PCI Hot Plug

The NC7770 ships with PCI Hot Plug support, which enables it to be replaced or added to a PCI Hot Plug compatible server without powering down the system. This feature provides increased system availability and non-stop serviceability in business-critical computing environments.

Network Management

Auto-negotiation

The NC7770 automatically senses and configures itself to the speed of the device to which it is attached. It also automatically configures for half or full duplex, depending on the duplex mode of the switch, hub, or router at the other end of the cable.

Management Support

Like all Compaq server adapters, the NC7770 ships with drivers and agents that can be managed from all versions of Compaq Insight Manager, including the new Compaq Insight Manger 7, as well as using any management application that supports SNMP.

Server Integration

Compaq's *SmartStart™* configuration utility includes setup support for the NC7770 so the adapter can be configured as part of the SmartStart configuration process. Compaq Insight Manager can recognize the NC7770 individually or in port-bonded teams, and can collect and report SNMP statistics on the adapter.

events.

Integrated Management Log (IML) support is provided by the NC7770 for critical event logging on Compaq servers.

Configuration Utilities

Each NC7770 ships with a suite of OS-tailored configuration utilities that allow the user to run initial diagnostics and configure adapter teams for Network Fault Tolerance, Transmit Load Balancing, or Switch-Assisted Load Balancing (802.3ad static-mode configuration only) in the Windows 2000 and Windows NT operating systems.

LED Indicators

Bracket LED indicators show link integrity, network activity, and network speed for easy troubleshooting.

Specifications

Compliance

IEEE 802.3i, 802.3u, 802.3x, 802.3ab, 802.3ad (static configuration mode only), 802.1p

PCI-X 1.0

PCI 2.2

ACPI v1.1a

General Specifications

Communications Processor	Broadcom 5701(h)
	10/100/1000 Mbps, Half- and full-duplex
On-board memory	96KB
Data path	64-bit/133MHz, compatible with 64/100, 64/66, 64/33 and 32/33
Interrupt levels	INTA
Bus architecture	PCI-X bus-mastering, compatible with existing PCI bus architectures
Connector	RJ-45
Distance	Up to 328 feet/100 meters
Wiring	Category 5 or higher UTP
Dimensions (LxW)	6.6 x 2.5 in/16.5 x 6.4 cm

Power and Environmental Specifications

Operating	Temperature	32° to 131° F/0° to 55° C
	Humidity	10% to 95% non-condensing
Non-operating	Temperature	–40° to 85° F/–40° to 185° C
	Humidity	5% to 95%
Power requirement		2A @ 5V max
Emissions standards		FCC Class B, VCCI Class B, BSMI Class A, CISPR 22 Class B, EN60950, EN 55022 Class B, EN55024, UL, Canada UL, CES-003 Class B
Safety compliance		CE Mark

Operating System Support

Windows 2000

Windows NT 4.0

Linux, Red Hat, Caldera, and SuSE distributions

Novell NetWare 4.x, 5.x, 6.x Server

Caldera UnixWare 7

Caldera OpenUnix 8

Caldera OpenServer 5

MS-DOS Client for unattended installation

Kit Contents

NC7770 PCI-X Gigabit Server Adapter
CD containing Drivers, User Guide, and Installation and Diagnostic Utilities
Quick Install Card
Product Quality Statement
Product Warranty Statement

Warranty

Maximum: The remaining warranty of the Compaq product in which it is installed (to a maximum three-year, limited warranty).

Minimum: One year limited warranty.

See Internet address http://www.compaq.com for overall information on Compaq Computer Corporation. For further information on Compaq products, contact Compaq Sales at 1-800-544-5255 or the Compaq Technical Support Center (post sales) at 1-800-386-2172. For customer support and information about Compaq and its products, call 1-800-OK-COMPAQ.

Compaq PCs use genuine Microsoft® Windows®
www.microsoft.com/piracy/howtotell

DA-11051 - World Wide - Version 1 - January 28, 2002

156

contents
Overview HP Installation and HP Care Pack Services TechSpecs

QuickSpecs

HP StorageWorks FCA2355 2 Gb Fibre Channel HBA

Product Description

FCA2355 2 Gb, Dual Channel, 64-bit/66 MHz PCI-to-Fibre Channel Host Bus Adapter (HBA) with an embedded small form factor (LC) optical interface.
Operating system support for this HBA is Windows® 2000, Windows NT® 4.0.
This HBA is supported on Windows 2000 and Windows NT platforms configured with the ma6000, ra8000, esa12000, ema12000, ema16000, Enterprise Virtual Array V2, XP, VA, and the Enterprise Backup Solution (EBS) offerings. For SAN switch support consult the SAN Design Guide at the following address:
http://www.StorageWorks SAN.com.

Models

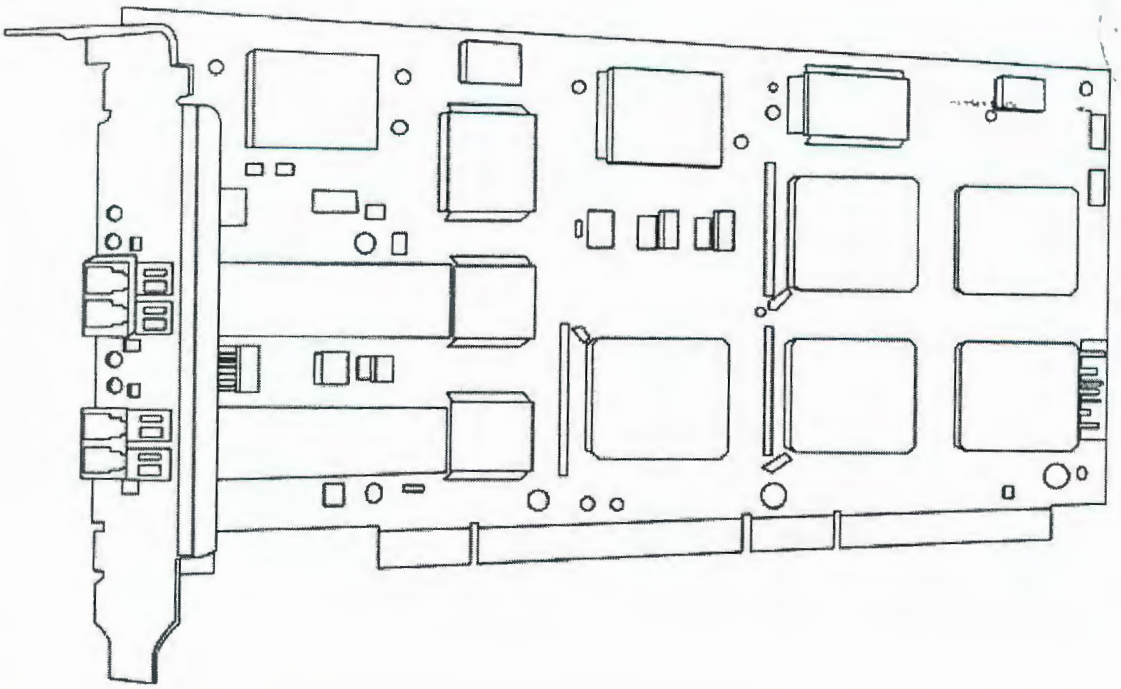
HP StorageWorks FCA2355 2 Gb Fibre Channel HBA	FCA2355 - StorageWorks 2 Gb, Dual Channel, 64-bit/66 MHz PCI to-Fibre Channel Host Bus Adapter for Windows 2000, Windows NT	308540-B21

Benefits at a Glance

- Automatic speed negotiation capability which allows compatibility with 1 Gb and 2 Gb devices
- Dual port HBA, provides two Fibre Channel optical connections in a single PCI slot
- Simultaneous full duplex 2 Gb/s Fibre Channel delivers up to 400MB/s/channel performance
- Provides the flexibility and broad interoperability needed for highly complex scalable SANs

Key Features

- Operating systems supported: Windows 2000 and Windows NT
- 64-bit PCI data and addressing
- Data transfer rate in full duplex mode is up to 400 Mb/s/Fibre Channel Connector
- Full fabric support using F_Port and FL_Port connections
- Backwards compatible with 1 Gb/s devices
- Full support for both FC service Class 2 and 3
- Support FC-Tape devices



contents

Overview HP Installation and HP Care Pack Services TechSpecs

HP Installation and HP Care Pack Services

Global Services

Global Services provides a three-year, limited warranty, fully supported by a worldwide network of resellers and service providers toll-free 7 x 24 hardware technical phone support for the duration of the warranty. In addition, available service offerings include a full range of HP Care Pack packaged hardware and software services:

- Installation and start up
- Extended coverage hours and enhanced response times
- System management and performance services

HP Service and Warranty Support

Additional Warranty protection and/or HP Installation packages can be purchased.

Software Product Services

- Stand-alone telephone support
- Rights to a new license
- Media and documentation updates

Hardware Product Services

- Installation services
- On-site Maintenance (includes warranty support)
- Response time upgrades during the warranty period
- Post-warranty coverage

For additional hardware installation and maintenance information please refer to the URLs listed below:
http://www.Hardware Services.com
http://www.Install Services.com

Warranty Upgrade Options

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

Additional Warranty protection and/or HP Installation packages can be purchased.

HP Care Pack Information and Installation Services

NOTE: Certain restrictions and exclusions apply. Consult the HP Customer Support Center for details.

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

3 years, 9x5, Next Business Day On-Site Coverage	FM-**XHW-36
3 years, 9x5, 4 –Hour Response On-Site Coverage	FM-**4HR-36
3 years, 24x7, 4-Hour response On-Site Coverage	FM-**724-36
Hardware Installation	FM-**INS-IN

For additional HP Care Pack (hardware & software) information, as well as orderable part numbers, please refer to the URL listed below:
http://h18005.www1.hp.com/services/carepaq/index.html

Contents
Overview HP Installation and HP Care Pack Services TechSpecs

TechSpecs

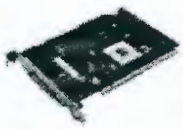
Environmental	**Temperature**	Operating	32° to 113° F/0° to 45° C
	Storage Temperature	Non-operating	-40° to 158° F/-40 to 70° C
	Relative Humidity	Operating	10% to 90% non-condensing
Mechanical Specifications	**Dimensions** (H x D)	Product	6.60 x 2.54 in/ 17.64 x 6.45 cm
Media		Multi-mode Optic	
Connector	**Optics**	One external small form factor multi-mode LC	
Ports		Two	
Power requirements	**Power**	6.5 watts	
Warranty	(3-0-0) Three-year parts exchange warranty. Additional Warranty protection can be purchased.		

NOTE: Certain restrictions and exclusions apply. Consult the HP Customer Support Center for details.

DA-11528 - World Wide - Version 4 - June 24, 2003

COMPAQ

SMART ARRAY 532 CONTROLLER



Manufacturer	COMPAQ
Mfg. Part #	225338-B21
ITEM#	9916
Unit Price	$672.07
Availability	In Stock
Buy	Add to Cart

Volume	Price	Ground S&H/unit
1 ~ 2	$672.07	
3 ~ 7	$660.20	$5.9
8 ~ 14	$652.64	$4.8
15 ~ 19	$645.01	$4.5
20 ~	$637.44	$4.4

Shipping and Handling: 5-8 Business Days -- $9.95

Product Spec.

Manufacturer:	Compaq
Quantity:	Single Pack
Controller Primary Interface:	Ultra2 SCSI (40 MBps)
Controller Primary Interface:	Ultra3 SCSI (160 MBps)
Type Slot/Interface:	64-bit PCI (66 MHz)
Primary Devices Supported:	20
Number of Channels:	2
Primary Port Placement:	Internal/External
Connector Style:	DB68 High Density
Cache Memory:	32 MB
Cache Memory:	Not Upgradeable
Sync Transfer Rate:	160 MBps
Misc Features:	RAID 0+1
Misc Features:	H/W Mirroring
Misc Features:	H/W Duplexing
Misc Features:	Bus Mastering
Misc Features:	Fault Monitoring
Misc Features:	RAID Array
Misc Features:	RAID 5
Misc Features:	RAID 0
Misc Features:	Installation Disk
Misc Features:	Utility S/W
Misc Features:	Installation Instructions
Misc Features:	RAID 1

Misc Features: Array Controller

[Disclaimer for Product Information]

QuickSpecs

hp Smart Array 532 Controller

Models

Smart Array 532 Controller

225338-B21
225338-291 (Japan)

- Dual SCSI channels (1 internal/1 external)
- ProLiant™ Integration
- Reliability
- Ultra3 SCSI
- 64-bit Architecture
- 64-bit PCI Bus Design
- Online Capacity Expansion
- Online RAID level Migration

What's New

Updated option support list, maximum storage support

Overview

The Smart Array 532 Controller (SA-532) is a 64-bit, 66 MHz dual SCSI channel PCI array controller for entry level hardware-based fault tolerance. Utilizing both SCSI channels (1 internal and 1 external) of the SA-532 allows you to configure up to 28 hard drives to store up to 4.1TB of storage per PCI slot. The SA-532 provides high reliability and increased performance over the Smart Array 431, thus providing excellent value and lowering the total server ownership cost. In addition, the SA-532 is data compatible with all Ultra320, Wide Ultra3 and Wide Ultra2 drives and servers, offering an unparalleled degree of investment protection. Designed and integrated with entry-level and workgroup ProLiant servers, this product provides worry-free data protection.
Note: The SA-532 is supported only in 3.3-volt PCI slots of all Ultra2 and Ultra3 servers. The SA-532 is not supported in 5-volt PCI slots. The SA-532 provides the best performance and capacity for RAID array controllers in entry-level and workgroup ProLiant servers or in any ProLiant server where hardware RAID is needed at an entry-level price point.

The Smart Array Advantage

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

- **Data Compatibility** - among all models of Smart Array controllers allows simple and easy upgrades any time needs for higher performance, capacity, and availability increase. Even successive generations of Smart Array controllers understand the data format of other Smart Array Controllers.
- **Consistent Configuration and Management Tools** - all

Smart Array products utilize a standard set of management and utility software. These tools minimize Total Cost of Ownership (TCO) by reducing training requirements and technical expertise necessary to install and maintain the ProLiant server storage.

- **Universal Hard Drive** - form factor is for use across multiple ProLiant servers, disk enclosures and storage systems. With compatibility across many enterprise platforms, you are free to deploy and re-deploy these drives to quickly deliver increased storage capacity, migrate data between systems, and easily manage spare drives.
- **Pre-Failure Warranty** - means *Insight Manager*ä not only reports when a drive is going to fail but allows replacement of failing drives prior to actual failure. For complete details, consult the HP Support Center or refer to your ProLiant Server documentation.

Key Features

Compatibility with all Ultra2, Ultra3, and Ultra320 LVD family products. In addition, a seamless upgrade to next generation HP high performance and high capacity mainstream Ultra3 Smart Array controllers.
Recovery ROM protects against a ROM corruption
Ultra3 SCSI technology delivers high performance and data bandwidth up to 160 MB/s bandwidth per channel
Mix-and-match LVD SCSI compatibility protects your investments and lets you deploy drives as needed
Dual SCSI channels allows for up to 4.1TB of storage per server slot (28 x 146.8GB Ultra320 hard drives)
Software consistency among all Smart Array family products: Array Configuration Utility XE (ACU-XE), Array Configuration Utility (ACU), Insight Manager (IM), Array Diagnostic Utility (ADU) and SmartStart.
64-bit, 66MHz PCI interface boosts bandwidth up to 533 MB/s total transfer rate
64-bit memory addressing supports servers with greater then 4 GB of memory
3.3 Volt Slot Support Only provides the latest in low-voltage, 64-bit support
32MB Memory optimizes performance and data throughput.
Note: 32 MB of DRAM used for code, transfer buffers, and non-battery backed read cache
Online Management Features: Online Capacity Expansion, Online RAID Level Migration, Online Stripe Size Migration, Online Spares (Global), User Selectable Expand and Rebuild Priority
Pre-Failure Warranty support for hard disk drives (requires Insight Manager).
Note: Pre-Failure Warranty is available on all Compaq Prosignia and ProLiant servers using Insight Manager 2.1 or higher, and covers Pentium® processors, ECC memory and server hard drives (except the 535 MB Fast-SCSI-2 hard drive) using Compaq IDA, IDA-2, Compaq SMART SCSI Array Controllers, Compaq SMART-2 Array Controllers or Compaq Smart Array Controllers. Certain restrictions and exclusions apply. Consult the HP Customer Support Center for details.

Product Highlights

Data Compatibility

Data compatibility among all models of Smart Array Controllers means customers can instantly upgrade their Smart Array products to get to higher performance, capacity and availability. Unlike competitive products, successive generations of Smart Array products

understand the data format of other Smart Array controllers, providing investment protection for your HP storage solution.

Performance

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

- Wide Ultra3 SCSI (160 MB/s bandwidth) per channel
- High-performance 64-bit architecture
- 64-bit, 66-MHz PCI bus (533 MB/s bandwidth)

Capacity

Given the rapid growth of user data, the SA-532 is a perfect companion to rapid expansion:

- Dual SCSI channels support up to 28 disk drives
- Up to 2 TB of storage per PCI slot

Availability

Provides increased server uptime by providing advanced storage functionality:

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

Fault Prevention

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

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

Fault Tolerance

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

- Distributed Data Guarding (RAID 5): This allocates parity data across multiple drives and allows simultaneous write operations. It is recommended for up to 14 hard drives.

- Drive Mirroring (RAID 1, 1+0): This allocates half of the drive array to data and the other half to mirrored data, providing two copies of every file. It is a high-performance RAID.

Fault Recovery

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

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

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

Ease of Use

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

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

Compatibility

Servers

For up to date compatibility, please see the following URL for complete Smart Array 532 compatibility and support information.
http://www.hp.com/products/smartarray
Note: Server must have 3.3 volt PCI slot(s) to support the SA-532 Controller.

Operating Systems

- NT® 4.0 Server
- NT 4.0 Enterprise Edition
- NT 4.0 Terminal Server
- Windows® 2000
- Windows 2000 Advanced Server
- NetWare® 4.x
- NetWare 5.x
- Linux® 32
- Linux 64
- AIX-5L (IA-64)
- UnixWare® 7.x
- OpenServer™ 5.x
- Solaris™
- OS/2

Software Suite

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

Insight Manager

- Powerful server and server options/storage manager tool
- Monitors over 1200 server parameters

Configuration/Diagnostic Utilities

- Array Configuration Utility XE (ACU-XE)

- Powerful Web based configuration utility for all Smart Array controllers
- Provides a graphical view of HP drive array configurations
- Allows for management of multiple arrays over a secure internet connection from anywhere in the world
- Easy to use Wizards for configuration
- Runs online on NT v4.0, Windows 2000 and NetWare

- Array Configuration Utility (ACU)

- Powerful configuration utility for all Smart Array controllers
- Provides a graphical view of HP drive array configurations
- Easy to use Wizards for configuration
- Runs online on NT v4.0, Windows 2000 and NetWare

- Options ROM Configuration for Arrays (ORCA)

- Rapid configuration during initial install of the OS

- Array Diagnostic Utility (ADU)

- Powerful diagnostic utility for all Smart Array controllers

Service & Support, *CarePaq*™ , and Warranty Information

Software Product Services

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

Hardware Product Services

- Installation services
- On-site maintenance (includes warranty support)
- Response time upgrades during the warranty period

- Post-warranty coverage
- RAID setup and performance consulting via statement of work

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

Warranty Upgrade Options

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

CarePaq Information

Sample part numbers:

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

** represents a two digit product specific code

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

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

Specifications

Protocol	Wide Ultra3 SCSI
SCSI Electrical Interface	Low Voltage Differential (LVD)
Drives Supported	Up to 28 Ultra320, Ultra3, and Ultra2 SCSI hard drives Note: The SA-532 will support all Ultra2 and Ultra3 servers, storage enclosures, and hard disk drives. The SA-532 does not support Single Ended hard disk drives, but does support Single Ended tape drives. (Single Ended refers to Wide Ultra SCSI and previous generations of the SCSI protocol).
SCSI Port Connectors	One external and one internal SCSI port
Data Transfer Method	64-Bit PCI bus-master

PCI Bus Speed	64-bit, 66-MHz PCI (533 MB/s maximum bandwidth)
PCI	3.3 volt CPI slot compatibility only Note: The SA-532 is not supported in 5 volt PCI slots.
Simultaneous Drive Transfer Channels	Two
Channel Transfer Rate	320 MB/s total; 160 MB/s per channel
Software upgradeable Firmware	Yes
Cache Memory	32 MB of DRAM used for code, transfer buffers, and non-battery backed read cache
Logical Drives Supported	32
Maximum Capacity	4.1TB (28 X 146.8 GB Ultra320 hard drives)
Memory Addressing	64-bit, supporting servers memory greater than 4 GB
RAID Support	RAID 5 (Distributed Data Guarding) RAID 1+0 (Striping & Mirroring) RAID 1 (Mirroring) RAID 0 (Striping)
Upgradeable Firmware	1-MB Flashable ROM
Disk Drive and Enclosure Protocol Support	Ultra2, Ultra3, and Ultra320
Dimensions (HxWxD)	15.25 x 11.0 x 4.25 in/38.71 x 27.92 x 10.79 cm
Weight	3.06 lb (1.39 kg)
Warranty	*Maximum:* The remaining warranty of the ProLiant server product in which it is installed (to a maximum three-year limited warranty) *Minimum:* One-year, on-site limited warranty *Pre-Failure Warranty:* Drives attached to the Smart Array Controller and monitored under Insight Manager are supported by a Pre-Failure (replacement) Warranty. For complete details, consult the HP Support Center or refer to your ProLiant Server Documentation.

Options

Hard Drives	***Wide Ultra3 SCSI Universal Drives – Hot Plug***	
	36.4-GB Wide Ultra3 SCSI 15,000 rpm Drive (1″)	232916-B22
	18.2-GB Wide Ultra3 SCSI 15,000 rpm Drive (1″)	188122-B22
	9.1-GB Wide Ultra3 SCSI 15,000 rpm Drive (1″)	188120-B22
	72.8-GB Wide Ultra3 SCSI 10,000 rpm Drive (1″)	232432-B22
	36.4-GB Wide Ultra3 SCSI 10,000 rpm Drive (1″)	176496-B22
	18.2-GB Wide Ultra3 SCSI 10,000 rpm Drive (1″)	142673-B22
	9.1-GB Wide Ultra3 SCSI 10,000 rpm Drive (1″)	142671-B22
	36-GB Wide Ultra3 SCSI 10,000 rpm Drives (1″), 10 pack	238617-B21
	18-GB Wide Ultra3 SCSI 10,000 rpm Drives (1″), 10 pack	202352-B21

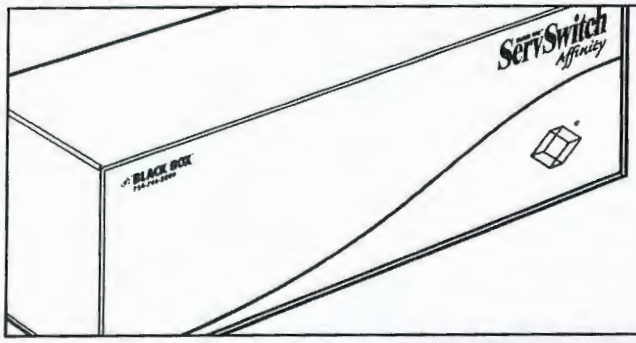
	Wide Ultra3 SCSI Drives – Non-Hot Plug	
	36.4-GB Wide Ultra3 SCSI 10,000 rpm Drive (1″)	176497-B21
	18.2-GB Wide Ultra3 SCSI 10,000 rpm Drive (1″)	142674-B21
	9.1-GB Wide Ultra3 SCSI 10,000 rpm Drive (1″)	142672-B21
	Ultra320 Universal Drives – Hot Plug	
	36.4GB 10,000 rpm, U320 Universal Hard Drive, 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: **This is a list of supported hard disk drives** (note that some drives may be discontinued).	
	Note: For complete compatibility information, refer to the SCSI Hard Drive Compatibility table located at http://www.compaq.com/products/servers/proliantstorage/drives-enclosures/docs/index.html	
Software	***SANWorks Virtual Replicator***	
	Note: For additional Virtual Replicator ordering information refer to http://www.compaq.com/products/StorageWorks/swvr/swvrorderinfo.html	
	License & Media (CD-ROM)	191802-B21
Universal Hot Plug Tape Drives	AIT 50 GB, Hot Plug (Carbon)	215487-B21
	AIT 35 GB, LVD Hot Plug (Carbon)	216886-B21
	20/40-GB DAT, Hot Plug (Carbon)	215488-B21
Storage Enclosures	Compaq *StorageWorks* Enclosure Model 4314T	190210-001
	Compaq StorageWorks Enclosure Model 4314T (Int'l)	190210-B31
	Compaq StorageWorks Enclosure Model 4314T (Japan)	190210-291
	Compaq StorageWorks Enclosure Model 4314R	190209-001
	Compaq StorageWorks Enclosure Model 4314R (Int'l)	190209-B31
	Compaq StorageWorks Enclosure Model 4314R (Japan)	190209-291
	Compaq StorageWorks Enclosure Model 4354R	190211-001
	Compaq StorageWorks Enclosure Model 4354R (Int'l)	190211-B31
	Compaq StorageWorks Enclosure Model 4354R (Japan)	190211-291
Related Products	HP RAID LC2 Controller	188044-B21
	HP RAID LC2 Controller (Japan)	188044-291
	HP Smart Array 5302/128 Controller	283552-B21
	HP Smart Array 5302/128 Controller (Japan)	283552-291
	HP Smart Array 5304/256 Controller	283551-B21
	HP Smart Array 5304/256 Controller (Japan)	283551-291

DA-10851 - World Wide - Version 8 - January 21, 2003

BLACK BOX® NETWORK SERVICES

Black Box Corporation • 1000 Park Drive • Lawrence, PA 15055-1018 • Tech Support: 724-746-5500 • **www.blackbox.com** • **e-mail: info@blackbox.com**

SERVSWITCH™ AFFINITY



Affordable many-to-many multiplatform KVM switching.

Key Features

- ***As many as 16 users have keyboard/mouse/video control over as many as 1024 PC, Sun, RS/6000, SGI, HP, and/or Alpha computers.***
- ***With additional converters, also supports Apple computers.***
- ***Easily expandable with plug-in Port Cards and flexible cabling.***
- ***Free lifetime firmware upgrades.***
- ***Supports video resolutions up to 1280 x 1024.***
- ***High levels of security, including passwords and access profiles.***
- ***Controlled through on-screen display, with additional keyboard commands and a terminal-based serial-port options menu.***
- ***Some models have redundant power supplies.***

Is your server room growing by leaps and bounds? Wouldn't it be nice to have a keyboard/video/mouse-switching system that could keep up with all the hardware, all the users, the constant changes, and the realities of your budget?

Our ServSwitch™ Affinity could be the one. It will support most major hardware platforms, including IBM® PS/2®, PC/AT®, and RS/6000®; Sun®; SGI™; HP® 700 and 9000 series; and Compaq® Alpha™. IBM type computers can use any keyboard mode and any of a variety of mouse types. Video can be any of several types at up to 1280 x 1024 resolution. With additional adapters, you can attach Apple® Macintosh® CPUs too—see **"What else you might need"** on page 4.

You can attach as many as 16 computers to a single unit or 1024 computers to a daisychained Affinity system. Either way, you can also attach up to 4, 8, or 16 independent users; more users can be connected, but they'll have to contend for access.

Here's how it works: Each ServSwitch Affinity has four slots for Port Cards. 0 x 4 Port Cards (product code KV1300C) have four CPU (computer) ports and a serial port only; 1 x 4 Cards (KV1301C) also have a KVM (user) port.

The Affinity chassis also has a fifth, top slot used for expansion purposes; the 16-User models have a matching sixth, bottom slot. 4-User models ship with a Terminator Card (KV1304C) installed in the expansion slot; you can swap in a 4-User Expansion Card (KV1305C) if you'll be daisychaining the Affinity. 8- and 16-User models, which are designed to be part of a daisychain, come without anything installed in the expansion slot(s). You need to purchase and install an 8-User Expansion Card (KV1306C) for each slot in order for the unit to work.

The only difference between the three 4-User Affinity models with single power supplies is which Cards they're preinstalled with; see the start of **"Ordering Information"** on page 5 for a list of which Cards come with each model.

You can add capacity to your Affinity system at any time by installing Port Cards in vacant slots or adding more chassis to a daisychain.

The Port Card's serial ports are used for terminal-based initial system configuration; they are also used to upgrade the Affinity's firmware (upgrades are free for the lifetime of the Affinity!).

The ServSwitch Affinity's main controls are its on-screen menus (with a full range of configuration and operating functions). These menus are augmented by a number of keyboard commands.

For added security, the Affinity supports password-protected access groups. Computers can belong to multiple groups, but users can only belong to one. Users will only be able to access the computers in their group.

When users do access computers, they'll have one of four assigned access levels: view only (no keyboard/mouse control), share (view access until current user becomes inactive, then add keyboard and mouse), control (sole control but others can view), or private (sole control, no one else can interrupt or view).

For mission-critical applications, we offer models of the Affinity with dual, redundant power supplies. If one power supply ever fails, the other can take on the entire load until a replacement supply can be installed.

6/26/2001 #22921

Specifications

Hardware Required: Monitor that supports your computers' highest video standard; in multiplatform applications, should be multisync model that can video from either composite sync or separate horizontal/vertical sync signals

Compliance: CE, FCC Part 15 Subpart J Class A, IC Class/ classe A

Standards:
- With original Serv cabling: VGA (color or monochrome/page white) video;
- With original Serv cabling (minimal) or coaxial cabling (recommended): SVGA and (with KV99MA adapter) Mac video;
- With coaxial cabling: XGA (color or monochrome), Sun, RS/6000, or SGI video

Interfaces:
- On CPU ports and user ports of Port Cards and IN 1 and OUT 1 ports of primary Expansion Cards:
  - Proprietary composite of:
    - IBM PS/2, PC/AT, or Sun compatible keyboard;
    - PS/2, RS-232 serial (except on user ports), or Sun compatible mouse; and
    - Video (see **Standards** above);
  - With the KV99MCON converter, also supports ADB (Mac compatible) keyboard and mouse ports;
  - IN 1 and OUT 1 also carry system-control signals;
- On Expansion Cards' other IN and OUT ports: Proprietary video composite (see **Standards** above);
- On serial ports of Port Cards: EIA/TIA RS-232 proprietarily pinned on RJ-12 ("6-wire RJ-11") connectors, DTE

Resolution: Up to 1280 x 1024, but will depend on the length of CPU and User Cables in your system

Serial (RS-232) Characteristics:
- Protocol: Asynchronous;
- Data format: 8 data bits, 1 stop bit, no parity (fixed);
- Data rate: 9600 or 57,600 bps

Maximum Distance:
- 20 ft. (6.1 m) of CPU or User Cable—possibly as much as 100 ft. (30.5 m) if Cable is coaxial, depending on CPUs, monitor, and video resolution—from any Affinity Port Card to any device attached to it;
- 100 ft. (30.5 m) of Expansion Cable between any two Affinity units;
- 50 ft. (15.2 m) of serial cable from the RS-232 port of any Affinity Port Card to a computer's serial port

User Controls:
- For system: Keyboard commands and on-screen menus;
- On Affinity chassis: Rear-mounted ON/OFF rocker switch(es); KV13xDA models: (2); All other models: (1);
- On all Expansion Cards (KV1305C and KV1306C): Board-mounted BUS/RING jumper;
- On 8-User Expansion Cards (KV1306C): (2) Board-mounted jumper blocks for user-port numbering

Indicators:
- All models: ON/OFF switch(es) are dark when ServSwitch Affinity is OFF, backlit when Affinity is ON;
- KV13xDA models: (3) Front-mounted power-supply status LEDs:
  - (1) for supply 1 (the upper transformer), lit while supply is outputting power;
  - (1) for supply 2 (the lower transformer), lit while supply is outputting power;
  - (1) for the Affinity chassis (marked "SYSTEM"), lit while either supply is outputting power unless internal diodes have failed

Connectors:
- All rear-mounted;
- On Affinity chassis: IEC 320 male power inlet(s): KV13xDA models: (2); All other models: (1);
- On all Affinity Port Cards (KV1300C and KV1301C): (4) DB25 female for CPU connections, (1) RJ-12 ("6-wire RJ-11") female for serial management;
- On 1 x 4 Port Cards (KV1301C): (1) DB25 female for user connections;
- On 4-User Expansion Cards (KV1305C):
  - (2) DB15 female: (1) for input to Port Cards in slots 1 and 2, (1) for input to Port Cards in slots 3 and 4;
  - (2) DB15 male: (1) for output from Port Cards in slots 1 and 2, (1) for output from Port Cards in slots 3 and 4
- On 8-User Expansion Cards (KV1306C):
  - (4) HD15 female:
    - (1) for input to Port Cards set as KVM 1/2 or 9/10;
    - (1) for input to Port Cards set as KVM 3/4 or 11/12;
    - (1) for input to Port Cards set as KVM 5/6 or 13/14;
    - (1) for input to Port Cards set as KVM 7/8 or 15/16;
  - (4) HD15 male:
    - (1) for output from Port Cards set as KVM 1/2 or 9/10;
    - (1) for output from Port Cards set as KVM 3/4 or 11/12;
    - (1) for output from Port Cards set as KVM 5/6 or 13/14;
    - (1) for output from Port Cards set as KVM 7/8 or 15/16

Maximum Altitude: 10,000 ft. (3048 m)

Temperature Tolerance: 32 to 113°F (0 to 45°C)

Humidity Tolerance: 5 to 80% noncondensing

Enclosure: Steel

Fuses: KV13xDA models: Autoresetting switch fuses that cut in when power surges exceed the maximum ratings of the chassis

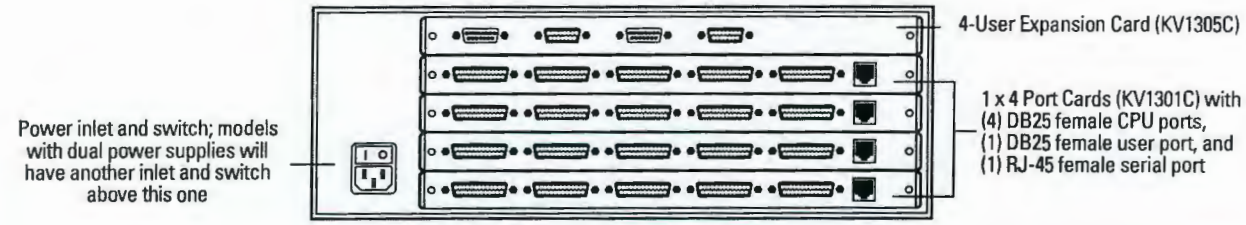
Power:
- Input: 90 to 264 VAC, 47 to 63 Hz, 700 mA from AC outlet(s) through included power cord(s) and inlet(s) into internal transformer(s): KV13xDA models: Dual transformers with separate AC inlets, electrically isolated from one another; All other models: Single transformer;
- Consumption: Up to 40 VA (40 watts)

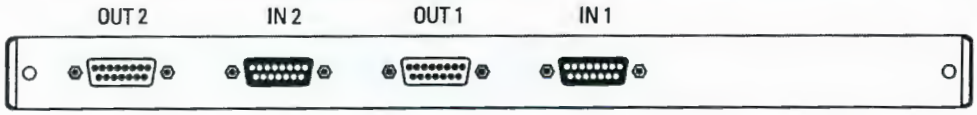
Size:
- KV139A and KV139DA chassis: 7"H (4U) x 16.7"W x 7"D (17.8 x 42.4 x 17.8 cm);
- All other Affinity chassis: 5.25"H (3U) x 16.7"W x 7"D (13.3 x 42.4 x 17.8 cm);
- Port Cards and Expansion Cards: 0.9"H x 13.9"W x 4.8"D (2.3 x 35.3 x 12.2 cm);
- Terminator Card (4-User models only): 0.4"H x 2.1"W x 0.8"D (1 x 5.3 x 2 cm)

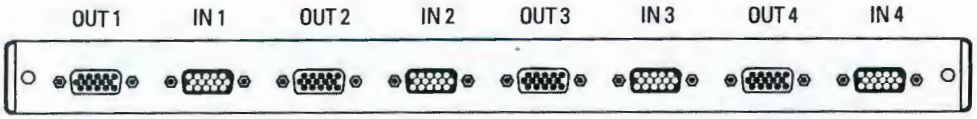
Weight:
- KV130A, KV130DA, KV138A, and KV138DA: 10.5 lb. (4.8 kg);
- KV132A: 12 lb. (5.5 kg);
- KV134A: 14 lb. (6.4 kg);
- KV139A and KV139DA: 11 lb. (5 kg);
- KV1300C, KV1301C, and KV1306C: 0.9 lb. (0.4 kg);
- KV1304C: 0.2 lb. (0.1 kg);
- KV1305C: 0.4 lb. (0.2 kg)

If you need to share access to a large number of CPUs, think about putting in an Affinity daisychain made up of 4-User Expansion Chassis (like the fully loaded one shown below) or 8- or 16-User Chassis. They come empty (no Cards installed), but you can install one Expansion Card (or two in the 16-User units) and add as many as four 0 x 4 or 1 x 4 Port Cards to them, giving you a maximum of four, eight, or sixteen user stations and sixteen CPUs attached to each unit. (Keep in mind that however many user stations a unit is designed for, only that many video paths can be open through that unit at a time. For example, a 4-User unit only has four video paths, so if there are already four users attached to a 4-User unit, and a user at another Affinity unit selects one of the 4-User unit's CPUs, one of the 4-User unit's users—and all other users on that slot—will be locked out until the new connection ends.)

The 8-User units look very similar to the 4-User unit shown here, but they accept only 8-User Expansion Cards like the one shown below. The 16-User Units accept two of the 8-User Expansion Cards. The 8-User Cards have jumper blocks that you can set to control which four KVM slots are used by the users attached to the Affinity chassis that the Card is installed in: KVM 1 through 4, 5 through 8, 9 through 12, or 13 through 16.





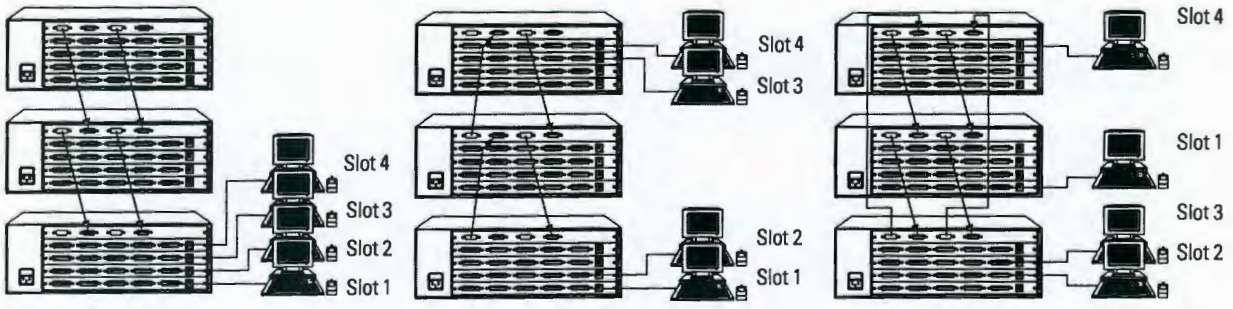


On the 4-User Expansion Cards (above, top), IN 1 and OUT 1 carry signals for the Port Cards in slots 1 and 2, while IN 2 and OUT 2 carry signals for the Port Cards in slots 3 and 4.

On the 8-User Expansion Cards (above, bottom), IN 1 and OUT 1 carry the signals for either KVM 1 and 2 or, if installed in the bottom slot of a 16-User unit, KVM 9 and 10; IN 2 and OUT 2 cary the signals for either KVM 3 and 4 or KVM 11 and 12; and so on. A pair of jumper blocks, mentioned above, determines which four KVM slots the four users on that Affinity chassis will use.

Because the control paths are carried on different connectors this way, you have maximum flexibility for designing your daisychain layout:

- If all of your users are on one Chassis, use the regular bus topology (below, left).
- If you have two users on one Chassis and two on another, use the "split bus" topology (below, middle).
- If your users are spread across several Chassis, use the ring topology (below, right).*



*It is always important to keep in mind that only one user at a time can use the bus that interconnects daisychained Affinity units, especially when you implement a ring topology. For example, when your Affinity units are interconnected in a ring, if any user on Slot 1 selects a CPU attached to an Affinity unit other than his own, no other Slot 1 user can select any CPUs.

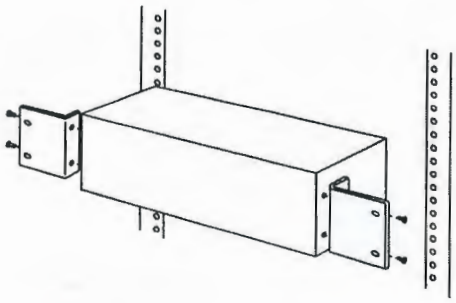
The complete package

- The ServSwitch Affinity, including any cards and blanking plates that are normally preinstalled with your model. (Blanking plates will cover all unused slots, as well as the slot on 4-User models that the tiny Terminator Card is installed in.)
- A power cord.
- *KV13xDA models only:* A second power cord.
- A 6-ft. (1.8-m) serial cable with RJ-12 ("6-wire RJ-11") plugs.
- An RJ-12 to DB9 modular adapter.
- A manual.

What else you might need

- CPU Adapter Cables, User Adapter Cables, and (if you're cascading) Expansion Cables.
- Keyboards, mice, and monitors for your users. If you're mixing platforms, we recommend true multiscan, multisync monitors capable of syncing to each CPU's video-output frequencies and compatible with all of the CPUs' video cards. Also, if one of the multiple platforms is IBM, the monitors must be able to accept both separate H/V sync and composite sync. (Such monitors are widely available.) We recommend that the monitors be able to display a maximum resolution of not less than 1280 x 1024 at a maximum refresh rate of not less than 75 Hz.
- An AC-power surge protector and uninterruptible power supply.
- Data-line surge protectors for the keyboard and mouse lines.
- *To attach an Apple Mac®:* A ServSwitch™ Micro Mac® Converter (product code KV99MCON), a G3™/G4™ or legacy Macintosh® style CPU-Extension Cable, and, if the Mac needs to see ID bits from its monitor, a Mac Video Adapter for ServSwitch (KV99MA).
- *If you purchase a 4-User Expansion Chassis or an 8- or 16-User Chassis:* Port Cards for your CPU and user-station connections.
- *To cascade a ServSwitch Affinity:* An Expansion Card.
- *To rackmount a ServSwitch Affinity:* A ServSwitch Affinity Rackmount Kit.

If you can use a screwdriver, you can install the Rackmount Kits.



Ordering Information

ITEM	CODE
ServSwitch Affinity	
4-User Expansion Chassis (Terminator Card installed, no Port Cards installed)	
Single power supply	KV130A
Dual power supply	KV130DA
4-User Standalone Chassis:	
2 Users by 8 CPUs (Terminator Card installed, 1 x 4 Port Cards installed in slots 1 and 2)	KV132A
4 Users by 16 CPUs (Terminator Card installed, 1 x 4 Port Cards installed in slots 1 through 4)	KV134A
8-User Chassis (no Cards installed)	
Single power supply	KV138A
Dual power supply	KV138DA
16-User Chassis (no Cards installed)	
Single power supply	KV139A
Dual power supply	KV139DA
Port Cards	
0 x 4 (No Users, Four CPUs)	KV1300C
1 x 4 (One User, Four CPUs)	KV1301C
4-User Terminator Card	KV1304C
4-User Expansion Card	KV1305C
8- and 16-User Expansion Card	KV1306C

Ordering Information (continued)

ITEM	CODE

NOTE: For CPU and User Cables, specify length by adding any of these suffixes to the product code (not all cables are available in all lengths):
"-0001" for 1 ft. (0.3 m, User Cables only),
"-0005" for 5 ft. (1.5 m),
"-0010" for 10 ft. (3 m),
"-0020" for 20 ft. (6.1 m),
"-0035" for 35 ft. (10.7 m),
"-0050" for 50 ft. (15.2 m),
"-0075" for 75 ft. (22.8 m), or
"-0100" for 100 ft. (30.5 m)

*You will need a **CPU Cable** for each CPU you attach:*

Standard CPU Cables, available in standard lengths up to 20 ft. (6.1 m)—Mac styles require keyboard/mouse conversion

IBM PS/2 style	EHN051
IBM PC/AT style	EHN048
Mac style with legacy DB15 video connectors	EHN215
Mac style with HD15 VGA video connectors for G3™, G4™, and similar models	EHN550

Coaxial CPU Cables—IBM and Sun styles available in all standard lengths, SGI and RS/6000 styles available in standard lengths up to 20 ft. (6.1 m), Mac styles require keyboard/mouse conversion

Universal IBM style	EHN282
Sun style with traditional 13W3 video connectors	EHN206
Sun style with VGA (HD15) video connectors	EHN515
SGI style	EHN500
RS/6000 style	EHN520
Mac style with traditional DB15 video connectors	EHN208
Mac style with HD15 VGA video connectors for G3, G4, and similar models	EHN560

ServSwitch™ Micro Mac® Converter to convert PS/2 kbd/mouse to ADB™ kbd/mouse signals	KV99MCON
For older Mac models that must see monitor ID: Mac® Video Adapter for ServSwitch™	KV99MA

*You will need a **User Cable** for each monitor/keyboard/mouse user station you attach:*

Regular (non-coaxial) User Cables, available in standard lengths up to 20 ft. (6.1 m)

IBM PS/2* style	EHN054
Sun style with VGA (HD15) video connector for multisync monitor	EHN059

Coaxial User Cables

IBM PS/2* style, available in all standard lengths except 1 ft. (0.3 m)	EHN283
Sun style with 13W3 video connector for Sun monitor, available in all standard lengths	EHN201
Sun style with VGA (HD15) video connector for multisync monitor, available in all standard lengths	EHN225
SGI style, 1 ft. (0.3 m) only	EHN501-0001
RS/6000 style, 1 ft. (0.3 m) only	EHN521-0001

*We no longer offer IBM PC/AT type User Cables for the ServSwitch Affinity, because its current firmware does not support serial mice, although it will still translate signals from PS/2 type mice into serial protocol for PC/AT CPUs.

Ordering Information (continued)

ITEM	CODE
You might also need:	
Expansion Cables for 4-User Units	
10 ft. (3 m)	KV140010
20 ft. (6.1 m)	KV140020
35 ft. (10.7 m)	KV140035
50 ft. (15.2 m)	KV140050
100 ft. (30.5 m)	KV140100
Expansion Cables for 8- and 16-User Units	
10 ft. (3 m)	KV180010
20 ft. (6.1 m)	KV180020
35 ft. (10.7 m)	KV180035
50 ft. (15.2 m)	KV180050
100 ft. (30.5 m)	KV180100
Replacement 6-wire straight-through-pinned flat-satin cable for serial management (specify length)	EL06MS-MM
Rackmount Kits	
To mount 4- or 8-User units in 19" Racks	RMK19A
To mount 4- or 8-User units in 23" Racks	RMK23A
To mount 4- or 8-User units in 24" Racks	RMK24A
To mount 16-User units in 19" Racks	RMK19A139
To mount 16-User units in 23" Racks	RMK23A139
To mount 16-User units in 24" Racks	RMK24A139
Surge protector for IBM PS/2 style keyboard and mouse lines (6-pin mini-DIN M/F)	SP519A-R2
Surge protector for IBM PC/AT style keyboard lines (5-pin DIN M/F)	SP518A-R2

Call Black Box Tech Support for help determining your best options for AC-power backup and protection.

Black Box offers the best warranty program in the industry—Fido Protection®. For more information, request **FaxBack 22512**.

Black Box Corporation * 1000 Park Drive * Lawrence, PA 15055-1018 * Tech Support: 724-746-5500 * **www.blackbox**

To bring to you the most accurate and up-to-date information, we have compiled this listing of UPDATED PRODUCTS. When you need the newest version of our products, consult this list to receive the newest information available, 24 hours a day!

Product Name	Codes	
2-Port Surface-Mount Housings		
Electrical Ivory	WP377-R2	6/
Gray	WP378-R2	6/(
Office White	WP272-R2	6/
Telco Ivory	WP278-R2	6/(
White	WP283-R2	6/(
4-Port Surface-Mount Housings		
Electrical Ivory	WP379-R2	6/
Gray	WP380-R2	6/(
Office White	WP273-R2	6/
Telco Ivory	WP277-R2	6/(
White	WP285-R2	6/(
10-/100-Mbps Autosensing Media Converters		
Multimode, 850-nm SC	LMC7002A-R2	3/(
Multimode, 850-nm ST	LMC7001A-R2	3/
Single-mode, Plus SC	LMC7004A-R2	3/(
Single-mode, Plus ST	LMC7003A-R2	3/(
16-Port Console Server	LS50116-R2	8/0
16-Port Console Server for U.K.	LS50116-AE-R2	8/(
20-Amp Rackmount Power Strips		
with Twist-lock Plug	SP471A-R2	5/
with Twist-lock Plug, On/Off Switch	SP470A-R2	5
with Twist-lock Plug, Surge Protection	SP473A-R2	5
with Twist-lock Plug, On/Off Switch, Surge Protection	SP472A-R2	5
23-inch Sliding Shelf	RM170-R2	6/(
24-inch Power Strip, 8-Outlets, 20-Amp	SP214A-R2	5/(

24-Port Console Server	LS50124-R2	8/0
24-Port Console Server for U.K.	LS50124-AE-R2	8/
2 Hour Drop-in Charger Tray for XTN Radio	53875	6/
2 to 1 Plug, 2.5A UK	POW20-R2	6/
230V Power Supply for AC043AE-R2, AC044AE-R2	PS044E-R2	3
6x4 Electronic SCSI Switch, Low-Voltage Differential	SW487A-R2	
Broadband Router	LR9501A	8/0
CAT5 100-MHz Patch Cables		
Crossover, 1-foot (0.3-meter)	EVCRB05-0001	5/
Crossover, 3-feet (0.9-meter)	EVCRB05-0003	5/
Crossover, 6-feet (1.8-meters)	EVCRB05-0006	5/
Crossover, 10-feet (3.0-meters)	EVCRB05-0010	5/
Crossover, 20-feet (6.0-meters)	EVCRB05-0020	5/

08/07/2002 #18038

Product Name	Codes	
CAT5e 350-MHz Patch Cables		
Crossover, 1-foot (0.3-meter)	EVCRB85-0001	5/
Crossover, 3-feet (0.9-meter)	EVCRB85-0003	5/
Crossover, 6-feet (1.8-meters)	EVCRB85-0006	5/
Crossover, 10-feet (3.0-meters)	EVCRB85-0010	5/
Crossover, 20-feet (6.0-meters)	EVCRB85-0020	5/
CAT5e Cross-Connect Block (110 Type), T568B	JPM051A-R2	6
CAT5 Economy Patch Panels		
16-Port, Universally Wired	JPM110A-R3	8
24-Port, Universally Wired	JPM111A-R3	8
32-Port, Universally Wired	JPM112A-R3	8
48-Port, Universally Wired	JPM113A-R3	8
96-Port, Universally Wired	JPM114A-R3	8
CAT5e Hinged Fold-Down Panels		
Rackmount	JPM202A-R2	6/
Wallmount	JPM201A-R2	6/
CertiFiber	TS655A-R2	1/0
Cisco ICRC Complete Curriculum	CISICRC.3	1/
Complete Cisco ICRC/ACRC Curriculum	CISIC&AC.3	1
Economy Series Ethernet Hubs		
8-Port	LE1060A-R2	1/
8-Port, w/PS114E	LE1060AE-R2	1/
16-Port	LE1061A-R2	1/
16-Port, w/PS115E	LE1061AE-R2	1/
Elite Server-Mount Cabinet Shelves		
Adjustable Fixed, Vented Heavy-Duty Shelf	RM403-R2	3
Fixed, Vented Server Shelf, 19-inch rails	RM399-R2	3
[illegible]	[illegible]	

Fixed, Vented Server Shelf, 23-inch rails ..... RM389-R2 .....3/
Fixed, Vented Server Shelf, 30-inch deep..... RM410-R2 .....3/

Express Ethernet Switches
12-Port, 10/100 Autosensing ..... LB9012A-R2 .....3/
7 RJ-45 ports, 1 pair SC ports..... LB9007A-SC-R2.....3/0
7 RJ-45 ports, 1 pair ST ports ..... LB9007A-ST-R2.....3/

Fiber Optic Adapters
FSD Duplex Receptacle, Key A to B..... FO201-R2.....6/
FSD Duplex Receptacle, Key M to S ..... FO201-R2.....6/

GigaBase CAT5e Patch Panels
16-Port, Universally Wired ..... JPM900A-R2 .....
24-Port, Universally Wired ..... JPM902A-R2 .....
32-Port, Universally Wired ..... JPM904A-R2 .....
48-Port, Universally Wired ..... JPM906A-R2 .....
96-Port, Universally Wired ..... JPM910A-R2 .....

GigaTrue CAT6 Patch Panels
24-Port, Universally Wired JPM610A-R2 8
48-Port, Universally Wired JPM612A-R2 8
96-Port, Universally Wired JPM614A-R2 8

Hard Leather Case ..... MR6045-200.....6/0

High-Speed Short-Range Modems
RS-422/449/530 Desktop ..... ME272AE-R3.....8/
V.35 Desktop, 115 VAC ..... ME270A-R3 .....
V.35 Desktop, 230 VAC ..... ME270AE-R3.....
X.21 Desktop, 230 VAC ..... ME271AE-R3.....8

Product Name	**Codes**	
Ladder Racks and Accessories		
Cable Retaining Post, Black	RM658-R2	8/
Cable Retaining Post, Gray	RM669-R2	8/
Foot Kit	RM649-R2	8/
Rack-to-Runway Mounting Plate, Black	RM653-R2	8/
Rack-to-Runway Mounting Plate, Gray	RM665-R2	8/
Support Bracket, Triangular, Black	RM654-R2	8/
Support Bracket, Triangular, Gray	RM667-R2	8/
Threaded Ceiling Kit	RM659-R2	8/
Matrix-Plus ServSwitch		
2 Users x 4 CPUs, Sun and PC	SW761A-R4	8/0
2 Users x 8 CPUs, Sun and PC	SW762A-R4	8/0
2 Users x 16 CPUs, Sun and PC	SW763A-R4	8/0
Mega Rack Power Strip	SP175A	6/0
Multi-Rate SDSL LAN Extender 200	LR0060A-R2	4/
Multimodem Iway Hopper-RS-232	MTA128ST-UK	

NetRack		
85"x19"x30", Beige, Plus 2 Shelves	RM505A-R3	5/
85"x19"x30", Black, Plus 2 Shelves	RM500A-R3	5/
Bottom Mount Tower Shelves, 2, Beige	RM507-R2	5
Bottom Mount Tower Shelves, 2, Black	RM502-R2	5
Caster Base, Beige	RM508-R3	5/0
Caster Base, Black	RM503-R3	5/0
Shelf, 25-inch, Vented, Beige	RM615-R2	5/
Shelf, 25-inch, Vented, Black	RM315-R2	5
Top Fan Panel, Beige	RM506-R3	5/0
Top Fan Panel, Black	RM501-R3	5/
NetRack Plus		
52-inch High, Beige	RM555A-R2	5/
52-inch High, Black	RM550A-R2	5/
78-inch High, Beige	RM565A-R2	5/
78-inch High, Black	RM560A-R2	5/
Casters	RM173-R3	5/0
Fixed Vented Shelf, 23-inch	RM172-R2	5
Palm-Sized Ethernet Switch, 5-Port	LB8405A-R2	3/
Palm-Sized Ethernet Switch, 8-Port	LB8408A-R2	3/
Pro 11 Series Wireless Ethernet		
8-dBi Omnidirectional Antenna	LW0029-R3	6/
13-dBi Directional Antenna	LW018A-R2	6
16-dBi Base Directional	LW019A-R2	6
24-dBi Directional Antenna	LW013-R2	6/
Extremely Low-Loss Extension Cable, 30-feet	LW0035-R2	8
Extremely Low-Loss Extension Cable, 50-feet	LW0036-R2	8
Rackmount Sync SHM Cards		
Balanced G.703 Interface, RS-530	ME270C-530-R2	8/0
Balanced G.703 Interface, V.35	ME270C-35-R2	8/
Unbalanced G.703 Interface, RS-530	ME275C-530-R2	8/0
Unbalanced G.703 Interface, V.35	ME275C-35-R2	8/
Relay/Digital I/O Card, PCI 32	IC903C-R2	3/
Remote Port USB, 1-Port	IC240A-R2	4/0
SCSI Matrix Switch, 2x2	SC120A-R2	8/
SCSI Matrix Switch, 4x2	SC122A-R2	8/

Product Name	Codes
Series 500 Branch Office Frame Relay Routers	
Base Model	LR1530A-R3 8/0
With 56K CSU/DSU	LR1531A-R2 8
With T1 CSU/DSU	LR1535A-R2 8/
With Universal WAN EU P/S	LR1530AEU-R3 8

Series 500 ISDN Routers
- Branch Office, S/T Interface EU P/S.....LR1560A-EU-STR2 8
- Branch Office, S/T Interface/Voice EU P/S.....LR1580A-EU-STR2 8
- Branch Office, U Interface LR1560A-U-R2 8
- Branch Office, U Interface/Voice.....LR1580A-U-R2 8
- Small Office, IP with PPP .....LR1500A-EU-R2.....8/
- Small Office, IP with PPP .....LR1500A-US-R3.....8/
- Small Office, IP with PPP, Voice, and Spoofing .....LR1520A-EU-R2.....
- Small Office, IP with PPP, Voice, and Spoofing .....LR1520A-US-R3.....

Series 5200 Router.....LR5200A-R2.....8/0

Series 6000 Routers
- Expandable, 14-Port, Dual Power Supply.....LR6114A-R3.....8/(
- Expandable, 14-Port, Single Power Supply .....LR6014A-R3.....8/

ServSwitch Affinity
- 1 User x 4 CPUs Card .....KV1301C-R2 .....8/(
- 1 User x 16 CPUs.....**KV131A**-R2.....8/(
- 2 User x 8 CPUs.....KV132A-R2.....8/(
- 4 User x 16 CPUs.....KV134A-R2.....8/(

T3 Fiber Optic Line Driver ST, Standalone
- 850-nm Multimode.....MT618A-ST-R2.....8/
- 1300-nm Single-Mode .....MT619A-ST-R2.....8/

Telephone Arm .....AC112A-R2.....6/(

Telephone Handset Lifter Accessory .....HL10 .....4/(

TV/VCR Connection Cables
- RG6 Screw-On, 6-feet, Black.....EJ203-0006 .....8/(
- RG6 Screw-On, 25-feet, Black.....EJ203-0025 .....8/(
- RG6 Slip-On, 3-feet, Black .....EJ205-0003 .....8/(
- RG6 Slip-On, 6-feet, Black .....EJ205-0006 .....8/(
- RG6 Slip-On, 12-feet, Black .....EJ205-0012 .....8/(
- RG6 Slip-On, 25-feet, Black .....EJ205-0025 .....8/(

Two-Way Radio, 1-Watt, 1-Channel, VHF.....XV1100.....1/

Two-Way Radio, 2-Watt, 6-Channel, UHF .....XU2600.....1/

Two-Way Radio, 2-Watt, 6-Channel, VHF.....XV2600.....1/

USB 2.0 4-Port Hub.....IC147A.....8/0

USB Director, 4-Port Hub.....IC165AE-R2 .....8/

Video Baluns
- 1-Way, RGB Video .....IC442A-R2.....6/
- 1-Way, Video Stereo Audio .....IC441A-R2.....6/
- 2-Way, Video Mono Audio.....IC443A-R2.....6

Video PTZ Balun .....IC450A-R2.....6/(

Wallmount Frame, 24-inch.....RM070A-R2.....5/(

Wallmount Frame, 38-inch.....RM069A-R2.....5/(

Wallmount Frame, 47-inch.....RM080A-R2.....5/(

Also available for you are:

UPDATED FAXBACKS , request **18021** . The newest information about our products.
UPDATED MANUALS , request **18014** . The newest information for our products.
PRICE CHANGES , request **17989** . Our competitive prices that fit your budget.
OLDER PRODUCTS , request **18007** . Discontinued products and recommended replacements.

FREE Expert Technical Support-24 Hours a Day!

Our expert staff is available with the answers you need, around the cloc
Call **724-746-5500** to speak with a Technician.
Or fax your questions to **1-800-321-0746.**

Fast, Reliable Delivery!

Next-day, second-day, or ground freight delivery available.
Black Box can even arrange same-day delivery.
Just call Customer Service, **877-877-BBOX (2269)** , to select th

Os equipamentos cotados são:

✓ KV138A	CHASSIS AFFINITY ARQUITETURA 8 USUARIOS
✓ KV1301C-R2	AFFINITY USER/CPU C 1 X 4 CARD
✓ KV1300C	SERVSWITCH AFFINITY - PLACA 0 USER X 4 CPUS
✓ KV1306C	SERVSWITCH AFFINITY HI-DENSITY EXPANS
✓ RMK19A-BB	SERVSWITCH AFFINITY KIT PARA RACK 19"
✓ KV180035	SERVSWITCH AFFINITY HI-DENS EXP CABLE
✓ EHN515-0035	CABO SERVSWITCH CPU SUN/HD15 COM 10,6M
✓ EHN382-0035	CABO SERVSWITCH CPU COAX PC COM 10,6M
✓ EHN382-0100	CABO SERVSWITCH CONSOLE COAX PC/PS2 COM 30,0M
✓ EHN383-0100	CABO SERVSWITCH CONSOLE COAX PC/PS2 COM 30,0M
✓ EHN225-0100	CABO SERVSWITCH CONSOLE SUN/HD15 COM 30,0M
✓ KV134A-R2	SERVSWITCH AFFINITY - 4 CONSOLES X 16 CPUS
✓ KV131A-R2	SERVSWITCH AFFINITY W/EXPANSION MODUL
✓ KV1305C	SERVSWITCH AFFINITY - PLACA DE EMPILHAMENTO
✓ KV140050	CABO DE EMPILHAMENTO PARA SERVSWITCH 15,2M

Atenciosamente

5º Tabelionato de Notas FRANÇA

São Paulo, 17 de julho de 2003

Wilson D. Batistela
Gerente Geral
Black Box do Brasil Ltda.

5o.Tabelionato de Notas - Jose Roberto Pacheco França - Tabelião
Av. João Dias, 2220-Santo Amaro - Fone 56416072 Fax 56053530 90432
Reconheco por semelhança firma de:
001-WILSON DONIZETE BATISTELA
VALIDO SOMENTE COM SELO DE AUTENTICIDADE - Doc. sem valor econ.
Carimbo:175796 18 DE JULHO DE 2003.
Total...:R$2,0 Em testemunho da verdade.
Conf...:FIRMA MARCIO CHAGAS BASTOS - ESCREVENTE

Simone Bifulco
Escrevente

AA045526

RQS nº 03/2005 - CN -
PMI - CORREIOS
0620
3685

contents
Overview Technical Specifications

QuickSpecs

hp CRT monitor s7500

Models **hp CRT monitor s7500** *261606-xxx*

contents
Overview Technical Specifications

Technical Specifications

Tube Type	Color, Conventional FST, multi-frequency				
Picture Tube Size (diagonal)	17-inch (43.18 cm)				
Viewable Image Area (diagonal)	16-inch (40.64 cm)				
Trio Dot Pitch	0.28 mm				
Horizontal Dot Pitch	0.24 mm				
Horizontal Frequency (kHz)	30 to 70 kHz				
Vertical Frequency (Hz)	50 to 140 Hz				
Maximum Pre-set Resolution	1280 x 1024 @ 60 Hz				
Preferred Flicker Free Resolution	1024 x 768 @ 85 Hz				
Preset Graphic Modes	1280 x 1024	1024 x 768	800 x 600	720 x 400	640 x 480
NOTE: All modes are non-interlaced unless specified otherwise.	@ 60 Hz	@ 85 Hz and 75 Hz	@ 85 Hz and 75 Hz	@ 70 Hz	@ 85 Hz, 75 Hz, 60 Hz
User-Modes	Yes, 8 modes				
Anti-Glare/Anti-Static	Yes				
AssetControl	Yes, supported				
Plug and Play	Yes				
Icon Based On-Screen Display Controls	Yes				
User Controls	**Brightness, Contrast**	Yes			
	Size and Positioning	Yes			
	Pincushion (barrel)	Yes			
	Trapezoid	Yes			
	Tilt (rotation)	Yes			
	Selectable Color temperature	Yes			
	Parallelogram	Yes			
	Pincushion Balance	Yes			
	Exit	Yes			

	Degauss	Yes
	Factory Reset/Recall	Yes
	Current Display Mode	Yes
Approvals/ Certifications	**UL/CSA/CUL Approval**	Yes
	ISO9241-3, -7, -8 VDT Guidelines Approval	Yes
	MPR-II Compliant	Yes, select models
	TCO '99	Yes, select models
	FCC Approval	Yes
	Microsoft WHQL Certified	Yes
	Energy Star Compliant	Yes
	CE	Yes
Maximum Pixel Clock Speed	110 MHz	
Power Supply	Universal; 100 to 240 V, 50 ± 3Hz and 60 ± 3Hz	
Maximum Power Rating	= 100 watts	
Low Power Sleep Mode	< 5 watts	
Signal Cable	15-pin miniature D-sub, attached, 4.9 feet (1.5 meters)	
Dimensions (H x W x D)	**Unpacked**	17 x 16.6 x 17.5 in (43.2 x 41 x 44.5 cm)
	Packaged	18.9 x 20.3 x 22.1 in (48 x 51.6 x 56.1 cm)
Weight	**Unpacked**	38 lb (17.23 kg)
	Packaged	46.2 lb (20.9 kg)
Operating Temperature (non-condensing)	50° to 95° F (10° to 35° C)	
Operating Humidity non-condensing)	20% to 80%	
Compatibility	Compaq Evo PCs and Thin Clients and Compaq D315 Business PC	
Warranty	Limited three-year parts and repair labor, one-year Service Provider labor and one-year on-site service warranty. 48 hour advanced exchange service available during warranty period. Certain restrictions and exclusions apply. For details, contact HP Customer Support.	

DA-11017 - U.S. - Version 2 - May 1, 2003

PRO 399/2003

24.664

SISTAB NO BREAKS
15 ANOS
CONDICIONANDO
ENERGIA
1988 - 2003

A SISTAB CONTRIBUI COM O PROGRAMA DE RECICLAGEM DE BATERIAS

A
COBRA SISTEMAS S/A
Estrada dos Bandeirantes, 7966 - Jacarepaguá
Rio de Janeiro - RJ

TRANSFORMADOR ISOLADOR COM CAIXA – 14 unidades

Modelo: Trafo Isolador 600 W com caixa

Potência de Utilização: **600 W**

Configuração: Monofásica

Tensão de Entrada: 110 V

Tensão de Saída : 220 V

Freqüência: 60 Hz

24.663

ANEXO INTEL

HARDWARE ADICIONAL

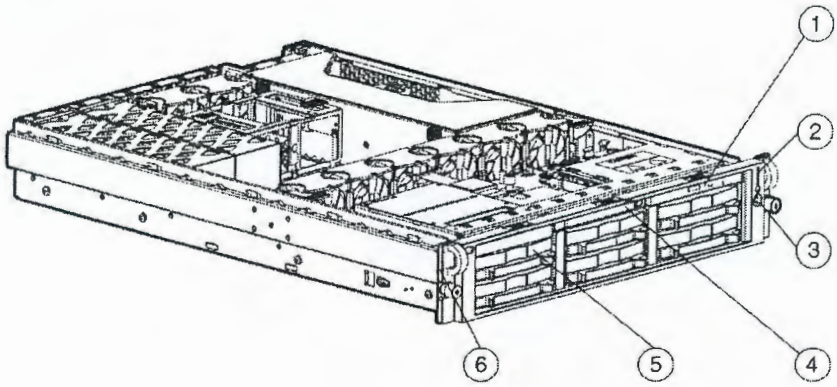
SERVIDORES MONITORAÇÃO DE REDE

NOTEBOOKS

COBRA Tecnologia S.A.
Estrada dos Bandeirantes 7966
CEP 22783-110 Rio de Janeiro RJ

QuickSpecs

Overview



1. 24X Max CD-ROM (with easy front ejection removal)
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 Ultra3/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 (available in North America only)
- 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/duol channel drive backplane
- Internal hot plug capacity 880.8 GB standard (6 x 146.8 GB 1" HD)
- 400-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 Global 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.

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_div/11063_div.HTML (Worldwide) http://www5.compaq.com/products/quickspecs/11063_na/11063_na.HTML (North America)	
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 available 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, and portables, and send alerts to Insight Manager 7 and other enterprise management applications in case of subsystem or environmental failures. For additional information about the Management Agents and other management products from, HP please visit the management 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 advanced configuration analysis, reporting and troubleshooting utilities used by HP and at your fingertips.
	Optional ProLiant Essentials Value Packs	Optional software offerings that selectively extend the functionality of an Adaptive Infrastructure to address specific business problems and needs: • Rapid Deployment Pack – an automated solution for multi-server deployment and provisioning, enabling companies to quickly and easily adapt to changing business demands. • Workload Management Pack – provides easier management of complex environments, improving overall server utilization and enabling Windows 2000 customers for the first time to confidently deploy multiple applications on a single multiprocessor ProLiant Server. • 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 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.

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.

Standard Features

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 closs 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 a custom solutions available through Foctory Express. Please contact a your local reseller or Account Manager.

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 ovailable 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

Models

DL380R03 X3.06-1MB/533, 1GB *333704-xx1*	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 X3.06-12KB/533, 1GB *310587-xx1*	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* NOTE: Available in NA only.	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-xx1*	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-xx1*	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)

Country Code Key	XX=00	US
	XX=01	Australia
	XX=03	UK
	XX=29	Japan
	XX=37	APD
	XX=42	EURO
	XX=AA	PRC

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) (NA)	313054-001
	Hot Plug AC Redundant Power Supply Module (IEC cord) (WW)	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, 1 User, V1.x (Japan) NOTE: This license allows 1 server ta be managed and deployed via the Deployment Server.	267196-291
	Rapid Deployment Pack, 10 Users, V1.x NOTE: This license allows 10 servers to be managed and deployed via the Deployment Server.	269817-B21
	Rapid Deployment Pack, 10 Users, V1.x (Japan) NOTE: TThis license allows 10 servers to be managed and deployed via the Deployment Server.	269817-291
	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
ocessor	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 ar 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

Options

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)	300682-B21
	NOTE: The 4096MB of Advanced ECC PC2100 DDR Memory kit (300682-B21) can only be used in 3.06GHz and faster models.	
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_div/11531_div.HTML (Worldwide) http://www5.compaq.com/products/quickspecs/11531_na/11531_na.HTML (North America)	

Options

Storage Controllers	Battery Backed Write Cache Enabler Option Kit	255514-B21
	Battery Backed Write Cache Enabler Option Kit (Japan)	255514-291
	Smart Array 532 Controller	225338-B21
	Smart Array 532 Cantroller (Japan)	225338-291
	Smart Array 5302/128 Controller	283552-B21
	Smart Array 5302/128 Cantroller (Japan)	283552-291
	Smart Array 5304/256 Controller	283551-B21
	Smart Array 5304/256 Cantroller (Japan)	283551-291
	Smart Array 6402/128 Controller	273915-B21
	Smart Array 5312 Controller	238633-B21
	Smart Array 5312 Controller (Japan)	238633-291
	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 Cache 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 as PCI Bus, PCI Peak Data Transfer Rate, SCSI Protocols supported, SCSI Peak Data Transfer Rate, Channels, SCSI Ports, Drives supported, Cache, RAID support, and additional information: http://www5.compaq.com/products/quickspecs/11063_div/11063_div.HTML (Smart Array 5i Plus) http://www5.compaq.com/products/quickspecs/10851_div/10851_div.HTML (Smart Array 532) http://www5.compaq.com/products/quickspecs/10640_div/10640_div.HTML (Smart Array 5300 Series) http://www5.compaq.com/products/quickspecs/11328_div/11328_div.HTML (Smart Array 5312) http://www5.compaq.com/products/quickspecs/11587_div/11587_div.HTML (Smart Array 6402) http://www5.compaq.com/products/quickspecs/11563_div/11563_div.HTML (Smart Array 641) http://www5.compaq.com/products/quickspecs/11563_div/11563_div.HTML (Smart Array 642) http://www5.compaq.com/products/quickspecs/10429_div/10429_div.HTML (SCSI Adapter) http://www5.compaq.com/products/quickspecs/11555_div/11555_div.HTML (U320 Adapter)	

Communications	NC3134 Fast Ethernet NIC 64 PCI Dual Port 10/100	138603-B21
	NC3135 Fost 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 Adopter	313881-B21
	NC7770 PCI-X Gigabit Server Adopter	244948-B21
	NOTE: Any NC31XX, NC61XX, NC71XX or NC77XX NIC can be used for redundancy with the embedded NC7781 Network Controller.	

Options

Redundant Options	DC Power Supply for the DL380 (48V) (WW) 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.	268290-B21
	DC Power Supply for the DL380 (48V) EMEA 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-B22) contains one power supply. Therefore, to convert to redundant DC power supplies, two must be purchased.	268290-B22
Redundant Options	Hot Plug AC Redundant Power Supply Module (NEMA cord) (NA)	313054-001
	Hot Plug AC Redundant Power Supply Module (IEC cord) (WW)	313054-B21
Management Options	Remote Insight Lights-Out Edition II (NA, LA) NOTE: USB Virtual Media Not Supported.	227251-001
	Remote Insight Lights-Out Edition II (EMEA) NOTE: USB Virtual Media Not Supported.	227251-021
	Remote Insight Lights-Out Edition II (ROW) 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.	227251-371
Security	HP/Atalla AXL600L SSL Accelerator Card for ProLiant Servers	524545-B21
	Compaq AXL300 Accelerator PCI Card (HW SSL Encryption) for ProLiant Servers	227933-B21

Options

Monitors

Essential Series	
Compaq S9500 CRT Monitor (19-inch, Carbon/Silver)	261615-XXX
Compaq S7500 CRT Monitor (17-inch, Carbon/Silver)	261606-XXX
Compaq S5500 CRT Monitor (15-inch Carbon/Silver)	261602-XXX
Compaq TFT1501 Flat Panel Monitor (15-inch, Carbon/Silver, North America)	301042-003
Compaq TFT1501 Flat Panel Monitor (15-inch, Carbon/Silver, Outside North America)	P4825D-XXX
Compaq TFT1701 Flat Panel Monitor (17-inch, Carbon/Silver, North America)	292847-003
Compaq TFT1701 Flat Panel Monitor (17-inch, Carbon/Silver, Outside North America)	P9019A-XXX
Advantage Series	
Compaq V7550 CRT Color Monitor (17-inch, Carbon/Silver)	261611-XXX
Compaq TFT1720 Flat Panel Monitor (17-inch, Carbon/Silver, North America)	295926-003
Compaq TFT1720 Flat Panel Monitor (17-inch, Carbon/Silver, outside North America)	D5064D-XXX
Compaq FT1720M Flat Panel Monitor (17-inch, Carbon/Silver, includes speaker, USB port, headphone, North America)	301958-003
Compaq TFT1720M Flat Panel Monitor (17-inch, Carbon/Silver, includes speaker, USB port, headphone, outside North America)	D5064P-XXX
Compaq TFT1520 Flat Panel Monitor (15-inch, Carbon/Silver, North America)	295925-003
Compaq TFT1520 Flat Panel Monitor (15-inch, Carbon/Silver, outside North America)	D5063D-XXX
Compaq TFT1520M Flat Panel Monitor (15-inch, Carbon/Silver includes speaker, USB port, headphone, North America)	301957-003
Compaq TFT1520M Flat Panel Monitor (15-inch, Carbon/Silver includes speaker, USB port, headphone, outside North America)	D5063P-XXX
Performance Series	
HP P930 CRT Monitor (19-inch, Flat-screen, Carbon/Silver, North America)	302268-003
HP P930 CRT Monitor (19-inch, Flat-screen, Carbon/Silver, Outside North America)	P909W-XXX
HP P1130 CRT Monitor (21-inch, Flat-screen, Carbon/Silver, North America)	302270-003
HP P1130 CRT Monitor (21-inch, Flat-screen, Carbon/Silver, Outside North America)	P4819-XXX
HP L1825 Flat Panel Monitor (18-inch, Carbon/Silver, North America)	303486-003
HP L1825 Flat Panel Monitor (18-inch, Carbon/Silver, Outside North America)	P9021W-XXX
HP L2025 Flat Panel Monitor (20-inch, Carbon/Silver, North America)	303102-003
HP L2025 Flat Panel Monitor (20-inch, Carbon/Silver, Outside North America)	P4831W-XXX
Compaq TFT1825 Flat Panel Monitor (18-inch, Carbon/Silver, North America)	296751-003
Compaq TFT1825 Flat Panel Monitor (18-inch, Carbon/Silver, Outside North America)	P9021A-XXX
Compaq TFT2025 Flat Panel Monitor (20-inch, Carbon/Silver, North America)	285550-003
Compaq TFT2025 Flat Panel Monitor (20-inch, Carbon/Silver, Outside North America)	P4831D-XXX
TFT5110R Flat Panel Monitor (Carbon)	281683-B21

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) (NA)	157770-002
HP StorageWorks 20/40-GB DAT DDS-4 Tape Drive, External (Int'l) (Carbon)	157770-B32
HP StorageWorks 20/40-GB DAT DDS-4 Tape Drive, External (Japan) (Carbon)	157770-292
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_div/10426_div.HTML (Worldwide)
http://www5.compaq.com/products/quickspecs/10426_na/10426_na.HTML (North America)

Internal and External DAT 72 Tape Backup Drives

HP StorageWorks DAT 72e External (US) (Carbon)	Q1527A
HP StorageWorks DAT 72e External (International) (Carbon)	Q1528A
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_div/11597_div.HTML (Worldwide)
http://www5.compaq.com/products/quickspecs/11597_na/11597_na.HTML (North America)

Internal and External AIT Tape Drives	
HP StorageWorks External AIT 35-GB, LVD Tape Drive (Carbon)	216885-001
HP StorageWorks External AIT 35-GB, LVD Tape Drive (Carbon) (Int'l)	216885-B31
HP StorageWorks External AIT 35-GB, LVD Tape Drive (Carbon) (Japon)	216885-291
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 os adapters, controllers, and cassettes, ond for an up-to-date listing of the latest O/S Support details, please see the following: http://www5.compaq.com/products/quickspecs/10712_div/10712_div.HTML (Worldwide) http://www5.compaq.com/products/quickspecs/10712_na/10712_na.HTML (North America)	
HP StorageWorks AIT 50-GB Tape Drive, External (Carbon) (NA)	157767-002
HP StorageWorks AIT 50-GB Tape Drive, External (Int'l) (Carbon)	157767-B32
HP StorageWorks AIT 50-GB Tape Drive, External (Japan) (Carbon)	157767-292
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_div/10425_div.HTML (Worldwide) http://www5.compaq.com/products/quickspecs/10425_na/10425_na.HTML (North America)	
HP StorageWorks External AIT 100-GB Tape Drive (Carbon)	249160-001
HP StorageWorks External AIT 100-GB Tape Drive (Carbon) (Int'l)	249160-B31
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_div/11062_div.HTML (Worldwide) http://www5.compaq.com/products/quickspecs/11062_na/11062_na.HTML (North America)	
External DLT Tape Drives	
HP StorageWorks External 20/40-GB DLT Drive (opal)	340744-B22
HP StorageWorks External 20/40-GB DLT Drive (opal) (Japan)	340744-292
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_div/10234_div.HTML (Worldwide) http://www5.compaq.com/products/quickspecs/10234_na/10234_na.HTML (North America)	
HP StorageWorks 40/80-GB DLT Tape Drive, External (Carbon) (NA)	146197-B22
HP StorageWorks 40/80-GB DLT Tape Drive, External (Carbon) (Japan)	146197-293
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_div/10658_div.HTML (Worldwide)	

http://www5.compaq.com/products/quickspecs/10658_na/10658_na.HTML (North America)

External LTO Ultrium Tape Drives

HP StorageWorks Ultrium 215 Tape Drive for ProLiant, External (Carbon) NA	Q1544A
HP StorageWorks Ultrium 215 Tape Drive for ProLiant, External (Carbon) Int'l	Q1545A

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_div/11678_div.html (Worldwide)
http://h18006.www1.hp.com/products/quickspecs/11678_na/11678_na.html (North America)

HP StorageWorks LTO Ultrium 230 Tape Drive, External (Carbon) NA	Q1516A
HP StorageWorks LTO Ultrium 230 Tape Drive, External (Carbon) Int'l	Q1517A

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_div/11415_div.HTML (Worldwide)
http://www5.compaq.com/products/quickspecs/11415_na/11415_na.HTML (North America)

HP StorageWorks Ultrium 460 Tape Drive for ProLiant, External (Carbon) NA	Q1519A
HP StorageWorks Ultrium 460 Tape Drive for ProLiant, External (Carbon) Int'l	Q1520A

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_div/11530_div.HTML (Worldwide)
http://www5.compaq.com/products/quickspecs/11530_na/11530_na.HTML (North America)

Internal and External SDLT Tape Drives

HP StorageWorks SDLT 110/220, External (Carbon) (NA)	192103-002
HP StorageWorks SDLT 110/220, External Int'l (carbon)	192103-B32
HP StorageWorks SDLT 110/220, External Japan (Carbon)	192103-292
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_div/10772_div.HTML (Worldwide)
http://www5.compaq.com/products/quickspecs/10772_na/10772_na.HTML (North America)

HP StorageWorks SDLT 160/320, External NA (carbon)	257319-001
HP StorageWorks SDLT 160/320, External Int'l (carbon)	257319-B31
HP StorageWorks SDLT 160/320, External Japan (carbon)	257319-291

NOTE: Please see the SDLT 160/320-GB Tape Drive QuickSpecs for additional options such as adapters, controllers, and media, and for an up-to-date listing of the latest O/S Support details, please see the following:
http://www5.compaq.com/products/quickspecs/11406_div/11406_div.HTML (Worldwide)
http://www5.compaq.com/products/quickspecs/11406_na/11406_na.HTML (North America)

External DAT Autoloader

20/40-GB DAT 8 Cassette Autoloader External (Opal)	166505-001
20/40-GB DAT 8 Cassette Autoloader External (Opal) (Int'l)	166505-B31
20/40-GB DAT 8 Cassette Autoloader External (Opal) (Japan)	166505-291

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_div/10518_div.HTML (Worldwide)

http://www5.compaq.com/products/quickspecs/10518_na/10518_na.HTML (North America)

AIT Autoloader

HP StorageWorks AIT 35 GB Autoloader, Rackmount (Carbon) (NA)	280349-001
HP StorageWorks AIT 35 GB Autoloader, Rackmount (Carbon) (Int'l)	280349-B31

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_div/11404_div.HTML (Worldwide)
http://www5.compaq.com/products/quickspecs/11404_na/11404_na.HTML (North America)

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 these kits, please see the following:
http://www5.compaq.com/products/quickspecs/10854_div/10854_div.HTML (Worldwide)
http://www5.compaq.com/products/quickspecs/10854_na/10854_na.HTML (North America)

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 (North America)
http://www5.compaq.com/products/quickspecs/11608_div/11608_div.HTML (Worldwide)

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 (North America)
http://www5.compaq.com/products/quickspecs/11438_div/11438_div.HTML (Worldwide)

MSL5052S2 - SDLT160 based departmental library up to 4 drives and 52 slots

MSL5052S2, 0 DRV, SDLT 160/320, RM Library	293402-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

24.644

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 (North America)
http://www5.compaq.com/products/quickspecs/11442_div/11442_div.HTML (Worldwide)

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 (North America)
http://www5.compaq.com/products/quickspecs/11625_div/11625_div.HTML (Worldwide)

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 (North America)
http://www5.compaq.com/products/quickspecs/11439_div/11439_div.HTML (Worldwide)

MSL5026S2 - SDLT160 based mid-range library up to 2 drives and 26 slots

MSL5026S2, 0 DRV, RM Library	293472-B21
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 ròuter option	293472-B25

NOTE: Please see the StorageWorks MSL5026SL Library QuickSpecs for additional information including Upgrade Kits, Accessories, ond SCSI Cable Kits and additional options needed for a complete solution at:
http://www5.compaq.com/products/quickspecs/11453_na/11453_na.HTML (North America)
http://www5.compaq.com/products/quickspecs/11453_div/11453_div.HTML (Worldwide)

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 (North America)
http://www5.compaq.com/products/quickspecs/11440_div/11440_div.HTML (Worldwide)

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 (North America)
http://www5.compaq.com/products/quickspecs/10860_div/10860_div.HTML (Worldwide)

MSL6000 and MSL5000 Add-on drives & accessories

Options

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 (North America) http://www5.compaq.com/products/quickspecs/10580_div/10580_div.HTML (Worldwide)	

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 (North America) http://www5.compaq.com/products/quickspecs/11050_div/11050_div.HTML (Worldwide)	

Options

Cluster Options	ProLiant Cluster HA/F100 for MSA1000 v2	252408-B22
	ProLiant Cluster HA/F100 for MSA1000 v2 (Japan)	252408-292
	ProLiant Cluster HA/F200 for MSA1000 v2	252409-B22
	ProLiant Cluster HA/F200 for MSA1000 v2 (Japan)	252409-292
	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 (North America) http://www5.compaq.com/products/quickspecs/11035_div/11035_div.html (Worldwide)	
	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 (North America) http://www5.compaq.com/products/quickspecs/11055_div/11055_div.html (Worldwide)	
	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 (North America) http://www5.compaq.com/products/quickspecs/10232_div/10232_div.html (Worldwide)	
	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 (North America) http://www5.compaq.com/products/quickspecs/11533_div/11533_div.html (Worldwide)	
	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 (North America) http://www5.compaq.com/products/quickspecs/11518_div/11518_div.html (Worldwide)	

External Storage - Rack	StorageWorks Enclosure Model 4314R (rack-mountable)	190209-001
	StorageWorks Enclosure Model 4314R (rack-mountable) (Int'l)	190209-B31
	StorageWorks Enclosure Model 4314R (rack-mountable) (Japan)	190209-291
	StorageWorks Enclosure Model 4354R (rack-mountable)	190211-001
	StorageWorks Enclosure Model 4354R (rack-mountable) (Int'l)	190211-B31
	StorageWorks Enclosure Model 4354R (rack-mountable) (Japan)	190211-291
	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	201723-B22
	MSA1000 Controller	218231-B22
	MSA Fibre Channel I/O Module	218960-B21
	MSA1000 Fabric Switch	218232-B21
	MSA1000 Fibre Channel Adapter (FCA) 2101	245299-B21
	HP StorageWorks msa hub 2/3	286763-B21
	NOTE: Please see the StorageWorks by Compaq Modular SAN Array 1000 QuickSpecs for additional options ond configuration information at: http://www5.compaq.com/products/quickspecs/11033_na/11033_na.HTML (North America) http://www5.compaq.com/products/quickspecs/11033_div/11033_div.HTML (Worldwide)	
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 chonnel HVD SCSI Module	262660-B21
	M2402 2 channel FC Madule	262661-B21
	MSL5000 Embedded Router Fibre Option Kit - Grophite	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 D14 50Hz	175990-B22
	EMA12000 S14 60Hz	175991-B21
	EMA12000 S14 50Hz	175991-B22
	MA8000 60Hz	175992-B21
	MA8000 50Hz	175992-B22
	EMA12000 Blue 60Hz	175993-B21
	EMA12000 Blue 50Hz	175993-B22
	NOTE: Options include controller, solution kits, ACS. MA8000/EMA12000 includes controller shelf, drive shelves and cabinet. Pockaging upgrade to RA8000/ESA12000.	
	NOTE: Please see the StorageWorks MA8000/EMA12000 QuickSpecs for FC Hubs, FC switches, platform software, host adopters, disks and options for complete solutions at: http://www5.compaq.com/products/quickspecs/10545_na/10545_na.HTML (North America) http://www5.compaq.com/products/quickspecs/10545_div/10545_div.HTML (Worldwide)	
StorageWorks Enterprise Modular Array 16000 FC	EMA16000 D14 50Hz (opal)	238792-B22
	EMA16000 D14 60Hz (opal)	238792-B21
	EMA16000 S14 50Hz (opal)	238791-B22
	EMA16000 S14 60Hz (opal)	238791-B21
	NOTE: Models include: Dual 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 (North America) http://www5.compaq.com/products/quickspecs/10812_div/10812_div.HTML (Worldwide)	

Options

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 (North America) http://www5.compaq.com/products/quickspecs/11003_div/11003_div.HTML (Worldwide)	
	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
UPS and PDU Power Cord Matrix	*Please see the UPS and PDU cable matrix that lists cable descriptions, requirements, and specifications for UPS and PDU units:* ftp://ftp.compaq.com/pub/products/servers/ProLiantstorage/power-protection/powercordmatrix.pdf. NOTE: This Web site is available in English only.	
Uninterruptible Power Systems – Rack	HP UPS R1500 XR (1440VA, 1340 Watt), Low Voltage (NA)	204404-001
	HP UPS R1500 XR (1500VA, 1340 Watt), High Voltage (Int'l)	204404-B31
	HP UPS R1500 XR (1500VA, 1340 Watt), Low Voltage (Japan)	204404-291
	HP UPS R3000 XR (2880VA, 2700 Watt), Low Voltage (NA)	192186-001
	HP UPS R3000 XR (3000VA, 2700 Watt), High Voltage (NA)	192186-002
	HP UPS R3000 XR (2400VA, 2250 Watt), Low Voltage (Japan)	192186-291
	HP UPS R3000 XR (3000VA, 2700 Watt), High Voltage (Japan)	192186-292
	HP UPS R3000 XR (3000VA, 2700 Watt), High Voltage (Int'l - detachable cord)	192186-B31
	HP UPS R3000 XR (3000VA, 2700 Watt), High Voltage (16A IEC309 Plug)	192186-B32
	HP UPS R3000 XR (3000VA, 2700 Watt), High Voltage (16A CEE 7/7 SCHUKO Plug)	192186-B33
	HP UPS R3000 XR (3000VA, 2700 Watt), High Voltage (16A BS-546 Plug)	192186-AR1
	Rack-Mountable UPS R6000 (6000VA, 6000 Watt) High Voltage (NA)	347207-001
	Rack-Mountable UPS R6000 (6000VA, 6000 Watt) High Voltage (Int'l)	347207-B31
	Rack-Mountable UPS R6000 (6000VA, 6000 Watt) High Voltage (Japan)	347207-291
	HP UPS R12000 XR N+x (200-240V) (WW-hardwired)	207552-B22
	NOTE: UPS R6000 has a hardwired input; and the UPS R12000 XR has a hardwired input and output connection.	

Options

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 (NA)	325361-001
	NOTE: The R12000 XR BackPlate Kit has a hardwired input.	
	R12000 XR BackPlate Receptacle Kit, (2) IEC-309R (WW)	325361-B21
	NOTE: The R12000 XR BackPlate 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.	
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) (NA, Japan)	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) (NA, Japan)	252663-D72
	HP Modular Power Distribution Units (mPDU), High Volt Model, 32A (200-240 VAC) (Int'l)	252663-B31
	HP Modular Power Distribution Units (mPDU), High Volt Model, 40A (200-240 VAC) (WW)	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) (WW)	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 additional options including shorter jumper cables and country specific power cards: http://www5.compaq.com/products/quickspecs/11041_na/11041_na.HTML (North America) http://www5.compaq.com/products/quickspecs/11041_div/11041_div.HTML (Worldwide)	

Options

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 (any 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-xx8

USB Easy Access Keyboard (Carbon) Country Key Code	Dash #	Description	Dash #	Description
	-008	US	-178	Arabic
	-038	UK	-188	Belgium
	-048	Germany	-218	Hungary
	-058	France	-228	Czech
	-068	Italy	-238	Solvac
	-078	Spain	-245	Polish
	-088	Denmark	-258	Russian
	-098	Norway	-298	Japan
	-108	Sweden/Finland	-338	Dutch
	-128	French Canadian	-358	Finish
	-138	Portugal	-B38	Int'l
	-148	Turkey	-B48	BHCSY
	-155	Greek		

USB Options	USB Easy Access Keyboard (carbonite)	DC168B#
	USB 2-Button Scroll Mouse (carbon)	195255-B25
	USB 2-Button Scroll Mouse (carbonite)	DC172B
	USB Floppy	304707-B21

Options

USB Easy Access Keyboard (Carbonite) Country Key Code	Dash #	Description	Dash #	Description
	A2M	ICELAND	ABT	HE
	AB0	TAWA	ABU	UK
	AB1	KOR	ABV	ARA
	AB2	PRC	ABX	FIN
	AB6	FRA	ABY	DEN
	AB7	GRK	ABZ	ITL
	AB8	TURK	AC0	BEL
	AB9	PORT	AC4	BRZ
	ABA	US	ACB	RUSS
	ABB	EURO	AKB	CZE
	ABC	FCAN	AKC	HUNG
	ABD	GR	AKD	POL
	ABE	SP	AKL	THAI
	ABF	FR	AKN	BHCSY
	ABH	NL	AKR	SLOV
	ABJ	Japan	ARK	ICELAND
	ABM	LA	B15	KAZ
	ABN	NOR	UUZ	SWISS
	ABS	SW		

Rack Builder	Please see the Rack Builder for configuration assistance at http://www.compaq.com/rackbuilder/

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, weight, and color: http://www5.compaq.com/products/quickspecs/10995_div/10995_div.HTML (Worldwide) http://www5.compaq.com/products/quickspecs/10995_na/10995_na.HTML (North America)	
	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_div/10366_div.HTML (Worldwide) http://www5.compaq.com/products/quickspecs/10366_na/10366_na.HTML (North America)	
	NOTE: For additional information regarding Rack Cabinets, please see the following URL: http://h18000.www1.hp.com/products/servers/proliantstorage/rack-options/index.html NOTE: This Web site is available in English only.	

Options

Rack Options for 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-B21) contains 10 each of (2U).	
	Rack Blanking Panels – Graphite (3U)	253214-B23
	NOTE: The Rack Blanking Panels (PN 253214-B21) contains 10 each of (3U).	
	Rack Blanking Panels – Graphite (4U)	253214-B24
	NOTE: The Rack Blanking Panels (PN 253214-B21) contains 10 each of (4U).	
	Rack Blanking Panels – Graphite (5U)	253214-B25
	NOTE: The Rack Blanking Panels (PN 253214-B21) 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.	

Options

Rack Options for Rack 9000 Series	Boying/Coupling Kit	120669-B21
	42U Side Panel	120670-B21
	NOTE: The 42U Side Panel (PN 120670-B21) supports the Compaq Rack 9142 and Compaq Rack 9842.	
	36U Side Panel	120671-B21
	NOTE: The 36U Side Panel (PN 120671-B21) supports the Compaq Rack 9136.	
	600mm Stabilizer Option Kit	120673-B21
	800mm Stabilizer Option Kit (Opal)	234493-B21
	NOTE: The 800mm Stabilizer Kit (PN 234493-B21) supports the Rack 9842 only.	
	9142 Extension Kit	120679-B21
	NOTE: The 9142 Extension Kit (PN 120679-B21) supports the Compaq Rack 9142 only.	
	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).	
	Rack Blanking Panels (2U)	189453-B22
	NOTE: The Rack Blanking Panels (PN 189453-B22) contains 10 each of (2U).	
	Rock 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 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 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 Rock 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	606-B21

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 Adjustoble Fixed Roil	332558-B21
	Cable Management D-Rings Kit	168233-B21
	Console Management Controller (CMC) Option Kit	203039-B21
	Console Monogement 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 2 port (100-230 VAC) (Int'l)	120206-B31
	Server Console Switch 1 x 2 port (100-230 VAC) (Japan)	120206-291
	Server Console Switch 1 x 4 port (100-230 VAC)	400336-001
	Server Console Switch 1 x 4 port (100-230 VAC) (Int'l)	400336-B31
	Server Console Switch 1 x 4 port (100-230 VAC) (Japan)	400336-291
	Server Console Switch 1 x 8 port (100-230 VAC)	400337-001
	Server Console Switch 1 x 8 port (100-230 VAC) (Int'l)	400337-B31
	Server Console Switch 1 x 8 port (100-230 VAC) (Japan)	400337-291
	Server Console Switch 2 x 8 port (100-230 VAC)	400338-001
	Server Console Switch 2 x 8 port (100-230 VAC) (Int'l)	400338-B31
	Server Console Switch 2 x 8 port (100-230 VAC) (Japan)	400338-291
	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
	Switch Box Connector Kit (high voltage) (Int'l)	144007-B33
	TFT5600 Rack Keyboard Monitor	221546-xx1
	Country Code Key (for TFT5600 RKM Rack Keyboard Monitor (PN 221546-xx1))	

XX = 001	US	XX = 091	Norway
XX = 031	UK	XX = 101	Sweden/Finland
XX = 041	Germany	XX = 111	Switzerland
XX = 051	France	XX = 131	Portugal
XX = 061	Italy	XX = 181	Belgium
XX = 071	Spain	XX = 291	Japan
XX = 081	Denmark	XX = B31	International

Local Access Cable Kit 232985-B21

1U Rack Keyboard & Drawer (Carbon) 257054-xx1

NOTE: The 1U Rack Keyboard & Drawer (PN 257054-xx1) is to be used with the Keyboards for Racks with Trackball (PN 158649-xxx).

Country Code Key (for 1U Rack Keyboard & Drawer (PN 257054-xx1))

XX = 001	US	XX = 091	Norway
XX = 031	UK	XX = 101	Sweden/Finland
XX = 041	Germany	XX = 111	Switzerland
XX = 051	France	XX = 131	Portugal
XX = 061	Italy	XX = 181	Belgium
XX = 071	Spain	XX = 291	Japan
XX = 081	Denmark	XX = B31	International

Input Device Adjustable Rails 287139-B21

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.

Input Device Telco Rail 287138-B21

NOTE: Input Device Adjustable Rails (287138-B21) are for use ONLY with the TFT5110R, TFT5600RKM and integrated keyboard/drawer which is used in mounting into third party racks.

Keyboard/Monitor/Mouse extension cables 169989-001

NOTE: For additional information regarding Rack Options, please see the following URL: http://h18000.www1.hp.com/products/servers/prolianstorage/rack-options/index.html
NOTE: This Web site is available in English only.

Rack Options for Third Party Cabinet Racks

Round hole rack cabinet rail kit 293052-B21

NOTE: Support for racks with round mounting holes (include HP Rack System /E and HP Systems) with an adjustment range of 24"- 36".

Options

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, validotion 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 Integratian Level 4 with 10 or more servers or storage enclosures	325733-888
	NOTE: Includes Level 2 Customer Intent plus customer defined cable management and naming convention, customer furnished image download, IP addressing, cluster configurations (SQL, External storage RAID). Quick restore creation, cd duplication, test reports, real-time reporting of server MAC address, password, RILOE). Customer access and validation through VPN (price/rack). NOTE: Available on ProLiant ML370 G3 Rack Models Only.	
	Factory Express Rack Integration Level 5 with 1 - 3 servers or storage enclosures	325732-888
	Factory Express Rack Integration Level 5 with 4 - 9 servers or storage enclosures	232541-888
	Factory Express Rack Integration Level 5 with 10 or mare servers or storage enclosures	325731-888
	NOTE: Includes Level 4 Customer Intent plus Custom SW layering ond extended test, Customer access, validation and control through VPN, Clustered racks with networking gear and/or external storage array, Start-up installation services custom quote. (price/rack). NOTE: Factory Express Engineered Solution Level 6 is a custom solutions available through Factory Express. Please contact a your local reseller or Account Manager. NOTE: Available on ProLiant ML370 G3 Rack Models Only.	

Service and Support Offerings (HP Care Pack Services)	*Hardware Services 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, 5-Day x 13-Hour Coverage, 3 Years (AP/EMEA Part Numbers)	U4544A U4544E
	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
	4-Hour On-site Service, 7-Day x 24-Hour Coverage, 3 Years (AP/EMEA Part Numbers)	U4545A U4545E
	Installation & Start-up Services	
	Hardware Installation (Canadian Part Number)	FP-LOINS-EC
	Hardware Installation (U.S. Part Number)	401792-002
	Hardware Installation (AP/EMEA Part Number)	U4554A U4554E
	Installation & Start-Up of a ProLiant server and Microsoft O/S per the Customer Description and/or	240014-002

Data Sheet. To be delivered on a scheduled basis 8am-5pm, M-F, excl. HP holidays. (U.S. Part Number)	
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 Microsoft or 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. (AP/EMEA Part Numbers)	U4555A U4555E
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 discretion, 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 Microsoft O/S SW Tech support offsite, onsite at HP's discretion, 8am-9pm, M-F 2hr response time excl. HP holidays. (AP/EMEA Part Numbers)	U4556A U4556E
Onsite HW support, 8am-9pm, M-F, 4hr response and Linux O/S SW Tech support offsite, onsite at HP's discretion, 8am-9pm, M-F 2hr response time excl. HP holidays. (U.S. Part Number)	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
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 (AP/EMEA Part Numbers)	U4558A U4558E
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 Microsoft O/S SW Tech support offsite, onsite at HP's discretion, 24x7 2hr response time incl. HP holidays. (AP/EMEA Part Numbers)	U4557A U4557E
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
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. (AP/EMEA Part Numbers)	U4559A U4559E
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 Windows 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,	239933-002

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.)	
24 x 7 HW, 4-hr response, Named HW engineer; 24 x 7 Silver Subsequent System Support for Windows NT, Windows 2000, Professional, Server or Advanced Server Operating System (6-3 Part Number for U.S.)	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
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

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

Storage

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) Option 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.

xternal 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_div/11033_div.HTML (Worldwide)
http://www5.compaq.com/products/quickspecs/11033_na/11033_na.HTML (North America)

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 (North America)
http://www5.compaq.com/products/quickspecs/Division/10233.html (Worldwide)

NOTE: For an up-to-date listing of the latest O/S Support details for each of the Tape Storage Systems listed below, please see the following:
http://www5.compaq.com/products/quickspecs/North_America/10809.html (North America)
http://www5.compaq.com/products/quickspecs/Division/10809.html (Worldwide)

NOTE: Please see the Smart Array 5i Controller QuickSpecs for additional information regarding supported options at:
...//www5.compaq.com/products/quickspecs/10890_NA/10890_NA.HTML (North America)
...//www5.compaq.com/products/quickspecs/10890_div.10890_div.HTML (Worldwide)

	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 Controller 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 Controller 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.
20/40-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

Storage

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

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
eakage 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
imum 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:

review typical system power ratings use the Active Answers Power Calculator which is available via the online tool located at URL:
.//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 Specifications

Power Cords (Nema 5-15P to IEC320-C13)	
Country	Standard Power Cord Part Number/Option Power Cord Part Number
JPN	139867-006/227100-291
US	163719-002/227099-001
Power Cords (IEC320-C13 to IEC320-C14)	Standard Power Cord Part Number/Option Power Cord Part Number
US	142263-003/142257-003
JPN	142263-003/142257-003
APD	142263-003/142257-003
EURO	142263-003/142257-003
PRC	142263-003/142257-003

TechSpecs

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% to 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

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	

TechSpecs

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

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

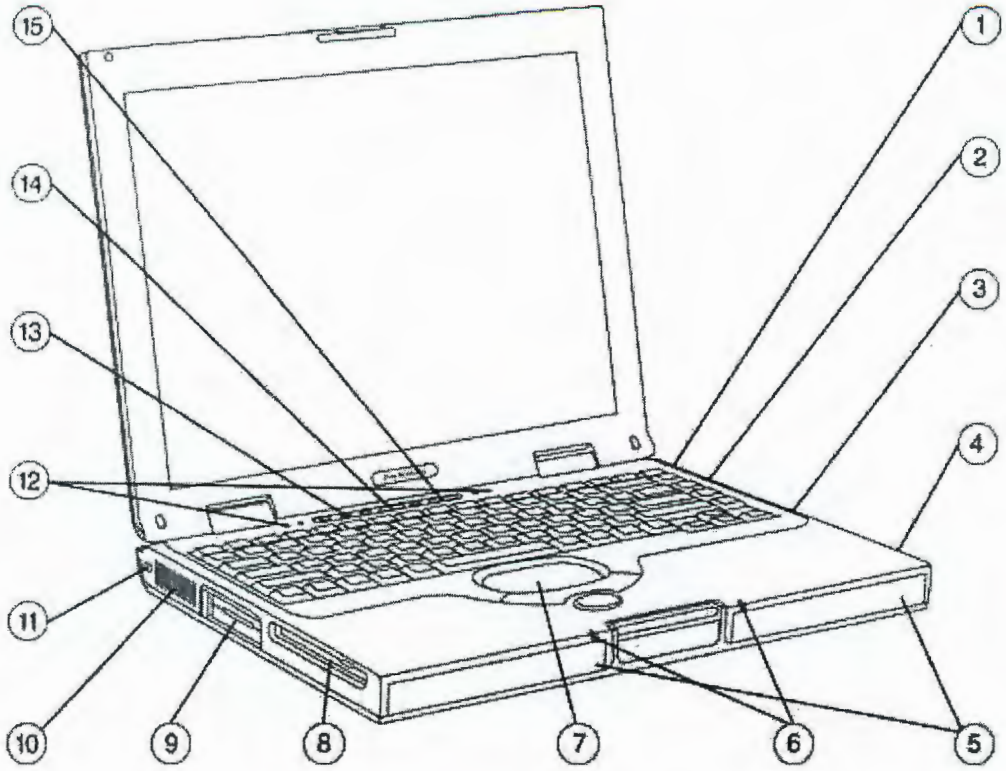
TechSpecs

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)

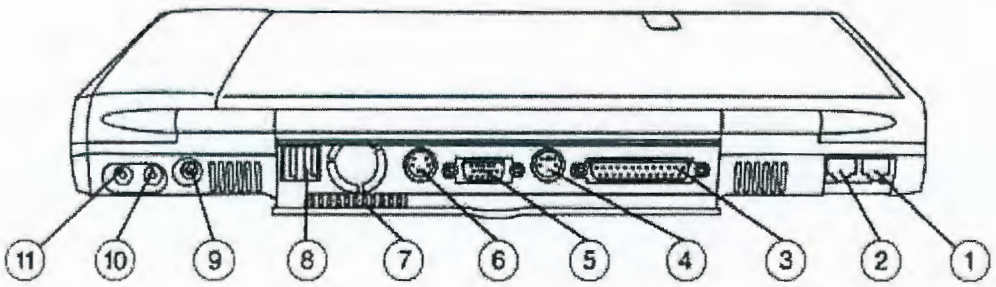
Video Controller	Controller Chip	ATI RAGE XL
	Video DRAM	8 MB Video SDRAM
	Data Transfer Method	32-bit PCI
	Support Resolution	Supported Color Depths:
	640 x 480	16.7M, 64K, 256, 16
	800 x 600	16.7M, 64K, 256, 16
	1024 x 768	16.7M, 64K, 256, 16
	1152 x 864	16.7M, 64K, 256, 16
	1280 x 1024	16.7M, 64K, 256, 16
	Connector	VGA

QuickSpecs

Compaq Evo Notebook N1020v



1. 1394
2. Infrared
3. Optical Drive
4. Battery
5. Stereo Speakers
6. System LEDs
7. Touchpad
8. Diskette Drive
9. PC Card Slot (1)
10. Kensington Lock
11. Air Vent
12. Keyboard LEDs
13. Easy Access Buttons
14. Power Button
15. Volume Control



1. RJ-11
2. RJ-45
3. Parallel
4. PS/2
5. VGA
6. S-video
7. Air Vent
8. USB
9. DC in
10 Audio in
11. Headphone

What's New

- Intel® Pentium® 4 processors – up to 2.4 GHz; Intel Celeron®

processors – up to 1.6 GHz
- 400-MHz bus
- 4X AGP Graphics
- MultiPort wireless communication options
- Touchpad

At A Glance

- Intel Pentium 4 processors – up to 2.4 GHz; Intel Celeron processors – up to 1.6 GHz
- 15-inch XGA and 14.1-inch XGA display
- Configurations as light as 6.6 lb (3 kg) weight (14-inch panel)
- 1.55 in (3.95 cm) thin
- 256 MB DDR SDRAM (266 MHz), Upgradeable to 1024 MB
- Up to 40 GB SMART hard drives
- Mini PCI modem and integrated NIC
- Full-size keyboard
- Microsoft® Windows® XP Pro and XP Home
- Includes a one-year, Worldwide Warranty. —Certain restrictions and exclusions apply. Consult the Compaq Customer Support Center for details.

What's Special

- Intel Pentium 4 processors
- All-in-one convenient design
- Latest USB 2.0 interface
- Wireless features thru award-winning MultiPort
- Common Docking Options

Overview Standard Features Options Memory Storage TechSpecs

Standard Features

Processor and Panel	15-inch color TFT XGA with 1024 x 768 resolution (up to 16.7M colors internal)	
	14.1-inch color TFT XGA with 1024 x 768 resolution (up to 16.7M colors internal)	
One of the following:	2.4 GHz Intel Pentium 4 processor with 512 KB L2 cache	
	2.0 GHz Intel Pentium 4 processor with 512 KB L2 cache	
	1.6 GHz Intel Celeron with 256 KB L2 cache	
Memory	Standard/Maximum	256 MB (266 MHz) DDR SDRAM (256 MB SODIMM in slot 1)
		576 1024 MB (266 MHz) DDR SDRAM (512 MB SODIMMs in slots 1 and 2)
	NOTE: Due to the non-industry standard nature of some third-party memory modules, we recommend Compaq branded memory to ensure compatibility.	
Communications	10/100 NIC is integrated on the system board	

	Type III Mini PCI 56K (V.92) modem **NOTE**: Designed only to allow faster downloads from V.92 compliant sources. Maximum achievable download transmission rates currently do not reach 56 KB/s, and will vary with line conditions. **NOTE**: Modem availability is subject to country regulatory approval	
Keyboard	88-key compatible keyboard with isolated, inverted-T cursor control keys, special feature hotkeys for instant access to power conservation, toggle between internal and external, or simultaneous displays, and control brightness and contrast.	
Easy Access Internet Buttons	The Evo Notebook N1020V comes with three Easy Access Buttons (EAB) designed to increase customer productivity by providing one-touch access to helpful Compaq information, favorite Internet destinations, or default e-mail application. The EAB portion of the keyboard deck also includes dedicated hardware volume control and a quick-launch button for CD/DVD play.	
Pointing Device	Touchpad with 4-way scroll	
PC Card Slots	One Type II PC Card Slot which supports both 32-bit CardBus and 16-bit PC Cards	
Storage	Fixed Diskette Drive	1.44 MB Diskette Drive
	Primary Hard Drive	40 GB or 30 GB or 20GB
	Fixed Optical Drive	DVD/CD-RW combo Drive DVD-ROM Drive CD-ROM Drive
Multimedia	JBL Pro Speakers with bass reflex and 16bit stereo sound Dedicated Hardware volume controls Headphone-out port Microphone in port Software MPEG1 support, MPEG2 and DVD 8X DVD/CD-RW Combination Drive (on select models) 8X DVD-ROM Drive with movie playback software (on select models) 24X CD-ROM Drive (on select models) S-video Port IEEE 1394 Port 4X AGP graphics 32 MB of DDR (Double Date Rate) SDRAM	
Interfaces	PC Card	One Type II
	Enhanced Parallel EPP/ECP	1

PS/2	1
S-Video	1
VGA	1
1394	1
Port Replicator	1
Headphone/Line-out	1
DC Power	1
RJ-11 (modem)	1
RJ-45 (NIC)	1
Infrared Port	1 (4 Mb/s support) (IrDA 4 MB compliant. IR performance will vary depending on performance of IR peripherals and application used.)
USB Port	2
LED status indicators	6

Graphics

ATI Radeon IGP 340M Integrated UMA architecture ATI 4X AGP 3D accelerator with 32-MB DDR shared video memory for increased color depth and graphics performance

Display (External)

Up to 32-bit per pixel color depth

Supports 640 x 480, 800 x 600, 1024 x 768, 1280 x 1024, 1400 x 1050, 1600 x 1200, or 2048 x 1536 resolutions up to 160-Hz refresh rate, dependent upon monitor capability, resolution and color depth settings

Display (Internal)

14.1-inch color TFT XGA with 1024 x 768 resolution (up to 16.7M colors internal)

15-inch color TFT XGA with 1024 x 768 resolution (up to 16.7M colors internal)

Operating System

Microsoft Windows XP Pro, or Microsoft Windows XP Home preinstalled

Software

Diagnostics for Microsoft Windows

DVD Playback Software

Compaq Security Management

Safety and Comfort Guide

Acrobat Reader

Reference Guide

Compaq Easy Access Button Software

System Recovery

Each unit is shipped with a CD kit for quick recovery (erases hard disk and restores manufacturer installed image) and software recovery (installs only selected standard software)

Security

Configuration Control Hardware

Memory Change Alert

Ownership Tag

Set-up Password

Power-On Password
DriveLock
Enabled for PC SmartCard options
Kensington Lock

Power Supply

External 90-watt AC adapter, power cord included.

Battery

Standard 8-cell Lithium-Ion battery.

The Evo Notebook N1020v provides over two hours of battery life using the standard 8-cell Lithium-Ion battery.

NOTE: Actual results may vary with product model, configuration, and individual usage. Compaq results of 2:20 (hr:min) were achieved running the Business Winstone 2001 Battery Mark™ 1.0 on a N1020Vv with a Intel Pentium 4 2.0 GHz CPU, 15-inch XGA panel, 256-MB RAM, 30-GB HDD, 8X DVD, 8-cell Lithium-Ion battery, and NIC/modem. System parameters were set according to eTesting Labs' recommendations: panel brightness 50%, hard drive timer three minutes.

NOTE: This test was performed without independent verification by eTesting Labs Inc. eTesting Labs Inc. makes no representations or warranties as to the result of the test. BatteryMark is a trademark of Ziff Davis Publishing Holdings Inc., and affiliate of eTesting Labs Inc., in the U.S. and other countries.

Power Conservation

Hibernation
Instant-on via Standby
Pop-ups with three presets
One custom level of power conservation
ACPI compliant

MultiPort

MultiPort is a flexible, innovative solution providing customers the ability to connect to their choice of wireless standards such as 802.11b or Bluetooth™. This can be achieved by simply changing out the high-performance wireless module, which is integrated into the top of the notebook. The award-winning MultiPort offers a cost effective means to migrate to future wireless standards as they become available.

Docking

Port replicator and Advanced Port Replicator. The sleek, new port replicator and advanced port replicator designs provide simple and convenient port management. Features include NIC pass through, USB, and a 1394 digital port. Compatible across multiple platforms for lower total cost of ownership.

Service and Support

Compaq Services includes a one-year, Worldwide Limited Warranty, pick-up or carry-in; upgraded warranty and toll-free 7 x 24 hardware technical phone support available.

NOTE: Certain restrictions and exclusions apply. Consult the Compaq Customer Support Center for details.

Naming Convention

The Etymology of a Model name:

Models

N1020vC160X420DC25E *P/N 470045-646*	**Display**	14.1-inch color TFT XGA
	Processor	1.60 GHz Celeron
	Cache Memory	256 KB, L2 Cache
	Standard Memory	256 MB (1 DIMM) 266 MHz DDR
	Maximum Memory	1024 MB (266 MHz) DDR
	Hard Drive	20 GB
	Optical Drive	24X CD-ROM Drive
	Communications	Type III Mini PCI 56K (V.92) modem, (LOM) integrated 10/100 NIC
	Graphics	ATI Radeon IGP 340M Integrated UMA architecture ATI 4X AGP 3D accelerator
	Audio	JBL Pro Speakers with bass reflex and 16-bit stereo sound
	Operating System	Microsoft Windows XP Home
	Warranty	One Year
N1020vP200X430VC25O *P/N 470045-647*	**Display**	14.1-inch color TFT XGA
	Processor	2.0 GHz Intel Pentium 4 processor
	Cache Memory	512 KB, L2 Cache
	Standard Memory	256 MB (1 DIMM) 266 MHz DDR
	Maximum Memoru	1024 MB (266 MHz) DDR
	Optical Drive	30 GB
	Hard Drive	8X DVD-ROM Drive
	Communications	Type III Mini PCI 56K (V.92) modem, (LOM) integrated 10/100 NIC
	Graphics	ATI Radeon IGP 340M Integrated UMA architecture ATI 4X AGP 3D accelerator
	Audio	JBL Pro Speakers with bass reflex and 16-bit stereo sound
	Operating System	Microsoft Windows XP Pro
	Warranty	One Year
N1020vP240X540WC25O *P/N 470045-648*	**Display**	15.0-inch color TFT XGA
	Processor	2.4 GHz Intel Pentium 4 processor

24.609

	Cache Memory	512 KB, L2 Cache
	Standard Memory	256 MB (1 DIMM) 266 MHz DDR
	Maximum Memoru	1024 MB (266 MHz) DDR
	Optical Drive	40 GB
	Hard Drive	DVD/CD-RW Combo Drive
	Communications	Type III Mini PCI 56K (V.92) modem, (LOM) integrated 10/100 NIC
	Graphics	ATI Radeon IGP 340M Integrated UMA architecture ATI 4X AGP 3D accelerator
	Audio	JBL Pro Speakers with bass reflex and 16-bit stereo sound
	Operating System	Microsoft Windows XP Pro
	Warranty	One Year
N1020vC160X420DC25O	**Display**	14.1-inch color TFT XGA
P/N 470047-364	**Processor**	1.60 GHz Celeron
	Cache Memory	256 KB, L2 Cache
	Standard Memory	256MB (1 DIMM) 266 MHz DDR
	Maximum Memoru	1024 MB (266 MHz) DDR
	Optical Drive	20GB
	Hard Drive	24X CD-ROM Drive
	Communications	Type III Mini PCI 56K (V.92) modem, (LOM) integrated 10/100 NIC
	Graphics	ATI Radeon IGP 340M Integrated UMA architecture ATI 4X AGP 3D accelerator
	Audio	JBL Pro Speakers with bass reflex and 16-bit stereo sound
	Operating System	Microsoft Windows XP Pro
	Warranty	One Year

Contents

Overview Standard Features Options Memory Storage TechSpecs

Options

Memory	512-MB (266 MHz) Memory Upgrade	269087-B25
	256-MB (266 MHz) Memory Upgrade	269086-B25
	128-MB (266 MHz) Memory Upgrade	269085-B25
Monitors	TFT8030 Flat Panel Color 18-inch (carbon/silver)	243362-001
	TFT7020 Flat Panel Color 17-inch with integrated speakers (carbon/silver)	253217-001
	TFT5015 Flat Panel Color 15-inch (carbon/silver)	234044-001
	TFT5030 Flat Panel Color 15-inch (carbon/silver)	228134-001
	V720 17-inch CRT (carbon/silver)	232944-001
	S720 17-inch CRT (carbon/silver)	239287-001
	V570 15-inch CRT (carbon/silver)	228113-001
Other Storage Devices	IBM 1-GB Microdrive (PC card Device)	247390-B25
	USB Disk-on-Key – 8 MB	249552-B25

24.608

Connectivity	Compaq Type II Mini PCI 56K (V.90) Modem		225640-B31
	Compaq Type II Mini PCI 56K (V.90) Modem plus 10/100 NIC Combo		225642-B31
	100BaseTX Ethernet Upgrade		225435-001
	1394 PC Card		177593-B25
	NOTE: Designed only to allow faster downloads from V.90 compliant sources. Maximum achievable download transmission rates currently do not reach 56 KB/s, and will vary with line conditions.		
Wireless Connectivity	802.11b MultiPort Wireless LAN module		283836-001
	Bluetooth MultiPort module		228057-B21
	Compaq WL110 Wireless LAN PC Card		191808-001
	Compaq WL510 Wireless Enterprise Access Point		216709-001
	Compaq WL410 Wireless SMB Access Point		191811-001
	Compaq WL310 Home Office Access Point		191813-001
	Compaq Range Extender Antenna		230268-B21
	CDPD WWAN PC Card (U.S. Only)		238111-001
Expansion Bases	Port Replicator		307648-001
	Advanced Port Replicator		307651-001
	External MultiBay		217388-001/002
	Monitor Stand		274407-B25
Power	Evo Notebook N1020v	8 Cell primary battery (4 Ah)	278418-B25
		8 Cell primary battery (4.4 Ah)	291369-B25
Common Power Solutions	External Battery Charger		265603-001
	External Battery Charger (Multiple Battery)		265604-001
	AC Adapter 90W		283884-001
	Aircraft Power Adapter 90W		291370-B25
Input Devices	External Enhanced III Keyboard (carbon)		118003-008
	Compaq 2 Button Mouse (carbon)		103180-B21
	USB 2 Button Scroll Mouse (carbon)		195255-B25
	External 10-Key Numeric Keypad (carbon)		294317-B21
	USB EZ Access Keyboard		222726-008
Security	Biometric PC Card		146805-B25
	Security Cable Lock		294316-B21
	Compaq Smart Card PC Card Reader		135646-B26
Useful Accessories	Compaq iPAQ Microportable Projector MP1200		261966-001
	Compaq iPAQ Microportable Projector MP3800		262839-001
	Compaq iPAQ Microportable Projector MP4800		257524-001

Lamp Module L20 for MP1200	266631-B24
Lamp Module L30 for MP3800	266633-B24
Home Theatre Kit HT150 for MP3800	292187-B24
Carrying Case for MP1200	295731-B24
Lamp Replacement Kit for MP1600	118052-001
Lamp Module for MP1800, MP1400	189789-001
Lamp Module for MP2800, MP2810	215464-001
Home Theater Kit HT110 for MP1410	246161-001
Multimedia Adapter & Remote Control Kit MMA110 for MP1410	246162-001
Multimedia Adapter & Remote Control Kit for MP1400, MP1800	174963-001
Deluxe Carrying Case for MP Series projectors	253364-001
Lamp Module for MP1410, MP1810	253365-001
Lamp Module L90 for MP4800	257892-001
Home Theater Kit HT180 for MP1200, MP4800	281729-001
CeilingMount Kit CM10 for MP1200, MP4800	281730-001
hp digital projector sb21	L1510A
hp digital projector xb31	L1511A
Ceiling Mount Kit for xb31	L1513A
M1-A to component/USB video cable for sb21, xb31	L1523A
M1-D to DVI/USB cable for sb21, xb31	L1529A
Lamp Module for sb21	L1515A
Lamp Module for xb31	L1516A

contents
Overview Standard Features Options Memory Storage TechSpecs

Memory

Compaq Evo N1020V

Standard Memory Plus Optional Memory

Support for up to 1024 MB of DDR SDRAM memory is available with the installation of optional DDR SDRAM Memory Kits.

Memory	Slot 1	Slot 2
256 MB	256 MB	–
384 MB	256 MB	128 MB
512 MB	512 MB	–
768 MB	512 MB	256 MB
1024 MB	512 MB	512 MB

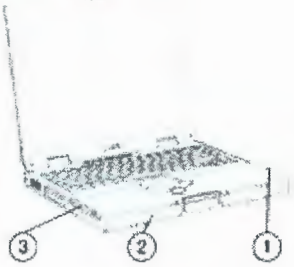
NOTE: This chart does not represent all possible memory configurations. Due to the non-industry standard nature of some third-party memory modules, we strongly recommend using only Compaq branded memory modules to ensure compatibility.

Following are memory options available from Compaq:

- 512-MB (266 MHz) Memory Upgrade 269087-B25
- 256-MB (266 MHz) Memory Upgrade 269086-B25
- 128-MB (266 MHz) Memory Upgrade 269085-B25

contents
Overview Standard Features Options Memory Storage TechSpecs

Storage



1. Dedicated optical drive
2. Primary hard drive
3. Dedicated floppy drive

Drive Support

System Drive Support	Quantity Supported	Drive Supported
1.44-MB Diskette Drive	1	Dedicated floppy drive
DVD/CD-RW Combo Drive	1	Dedicated optical drive
DVD-ROM Drive	1	Dedicated optical drive
Max CD-ROM Drive	1	Dedicated optical drive
Hard Drives		
40-GB SMART Hard Drive	1	Dedicated hard drive bay
30-GB SMART Hard Drive	1	Dedicated hard drive bay
20-GB SMART Hard Drive	1	Dedicated hard drive bay

contents

Overview Standard Features Options Memory Storage TechSpecs

TechSpecs

System Unit	**Dimensions** (H x W x D)	15-inch and 14.1-inch TFT panel displays	1.55 x 12.89 x 10.53 in (3.95 x 32.75 x 26.75 cm)
	Weight With P4 processor	14 inch: LCD, DVD or CD-ROM, 1 SODIMM	6.82 lb (3.1 kg)
		15 inch LCD, DVD or CD-ROM, 1 SODIMM	7.09 lb (3.2 kg)
	Weight With Celeron processor	14 inch: LCD, DVD or CD-ROM, 1 SODIMM	6.60 lb (3 kg)
		15 inch LCD, DVD or CD-ROM, 1 SODIMM	6.87 lb (3.12 kg)

NOTE: * = Weight varies by configuration.

Stand-Alone Power Requirements	Nominal Operating Voltage (Li-Ion)	14.4 V (8-cell)

		Average Operating Power	29.7 W Desktop
		Peak Operating Power	80 W on AC
			55 W on DC
		Power in suspend mode	< 1000 mW
		Power in hibernation mode	< 100 mW
	Power Supply	Rated Input Voltage	100 to 240 VAC
		Rated Input Current	< 1.5 A
		Rated Frequency	50 to 60 Hz
	Temperature	Operating	50° to 95° F (10° to 35° C)
		Non-operating	14° to 140° F (–10° to 60° C)
	Relative Humidity	Operating	10% to 90% relative humidity, non-condensing
		Non-operating	5% to 90% relative humidity, 101.6° F (38.7° C) Maximum wetbulb temperature
	Shock	Operating	10 G, 11 ms, half-sine
		Non-operating	60 G, 11 ms, half-sine
	Vibration	Operating	0.5 G zero-to-peak, 10 to 500 Hz, 0.25 oct/min sweep rate
		Non-operating	1.0 G, zero-to-peak, 10 to 500 Hz, 0.5 oct/min sweep rate
	Maximum Altitude (unpressurized)	Operating	0 to 10,000 ft (0 to 3,048 m)
		Non-operating	0 to 30,000 ft (0 to 9,144 m)
14.1-Inch Color TFT XGA Display	**Dimensions** (HxW)	11.22 x 8.46 in (28.5 x 21.5 cm)	
	Diagonal Size	14.1 in (35.81 cm)	
	Mounting	Internal Panel Supports, Side Mounted	
	Number of Colors	Up to 16.8M	
	Contrast Ratio	150:1	
	Brightness	120nt typ	
	Pixel Resolution	Pitch	0.264 x 0.264 mm
		Format	1024 x 768
		Configuration	RGB stripe
	Backlight	Edge Lit	
	Character Display	80 x 25	
	Total Power Consumption	4.2W	
15-Inch Color TFT SXGA+ Display	**Dimensions** (H x W)	11.8 x 9 in (30.4 x 22.8 cm)	
	Diagonal Size	15 in (38 cm)	

	Mounting	Internal Panel Supports, Side Mounted	
	Number of Colors	Up to 16.8M	
	Contrast Ratio	150:1	
	Brightness	150nt typ	
	Pixel Resolution	Pitch	0.218264 x 0.218264 mm
		Format	1400 x 1050
		Configuration	RGB stripe
	Backlight	Edge Lit	
	Character Display	80 x 25	
	Total Power Consumption	5.75W	
15-Inch Color TFT XGA Display	**Dimensions** (H x W)	11.8 x 9 in (30.4 x 22.8 cm)	
	Diagonal Size	15 in (38 cm)	
	Mounting	Internal Panel Supports, Side Mounted	
	Number of Colors	Up to 16.8M	
	Contrast Ratio	150:1	
	Brightness	150nt typ	
	Pixel Resolution	Pitch	0.297 x 0.297 mm
		Format	1024 x 768
		Configuration	RGB stripe
	Backlight	Edge Lit	
	Character Display	80 x 25	
	Total Power Consumption	5.0W	
Hard Drives			
60-GB	**Capacity**	60 GB	
	Drive Weight	0.34 lb (155 g)	
	Height	0.374 in (9.5 mm)	
	Width	70 mm	
	Interface	ATA-5	
	Transfer Rate	Synchronous (maximum)	100 MB/s (Drive Capability)
		Security	ATA Security
	Seek Time (typical reads, including settling)	Single Track	2.5 ms
		Average	13 ms
		Maximum	23 ms
	Rotational Speed	5400 rpm	
	Logical Blocks	117,210,240	
	Operating Temperature	41° to 131° F (5° to 55° C)	
	Features	Security	ATA Security
40-GB	**Drive Weight**	0.21 lb (95 g)	
	Capacity	40 GB	

	Height	0.374 in (9.5 mm)	
	Width	2.75in (70 mm)	
	Interface	ATA-5	
	Transfer Rate	Synchronous (maximum)	100 MB/s (Drive Capability)
		Security	ATA Security
	Seek Time (typical reads, including settling)	Single Track	3.0 ms
		Average	13 ms
		Maximum	25 ms
	Rotational Speed	4200 rpm	
	Logical Blocks	78,140,160	
	Operating Temperature	41° to 131° F (5° to 55° C)	
30-GB	**Drive Weight**	0.22 lb (99 g)	
	Capacity	30 GB	
	Height	0.374 in (9.5 mm)	
	Width	2.75 in (70 mm)	
	Interface	ATA-5	
	Transfer Rate	Synchronous (maximum)	100 MB/s (Drive Capability)
		Security	ATA Security
	Seek Time (typical reads, including settling)	Single Track	2.5 ms
		Average	12 ms
		Maximum	23 ms
	Rotational Speed	4200 rpm	
	Logical Blocks	58,605,120	
	Operating Temperature	41° to 131° F (5° to 55° C)	
20-GB	**Drive Weight**	0.21 lb (95 g)	
	Capacity	20 GB	
	Height	0.374 in (9.5 mm)	
	Width	2.75 in (70 mm)	
	Interface	ATA-5	
	Transfer Rate	Synchronous (maximum)	100 MB/s (Drive Capability)
		Security	ATA Security
	Seek Time (typical reads, including settling)	Single Track	2.5 ms
		Average	12 ms
		Maximum	23 ms
	Rotational Speed	4200 rpm	
	Logical Blocks	~ 39,070,080	
	Operating Temperature	41° to 131° F (5° to 55° C)	

Diskette Drive	**Diskette Size**	3.5 in	
	Activity Indicator	On system	
	Height	0.5 in (12.7 mm)	
	Bytes per Sector	512	
	Sectors per track	High density	18 (1.44 MB)/15 (1.2 MB)
		Low density	9
	Tracks per side	High density	80 (1.44 MB)/80 (1.2 MB)
		Low density	80
	Read/Write heads	2	
	Access Times	Track-to track (high/low)	3 ms/6 ms
		Average (high/low)	94 ms/174 ms
		Settling time	15 ms
		Latency average	100 ms
External AC Adapter	**Weight**	0.85 lb (0.385 kg)	
	Power Supply (Input)	Operating Watts	90
		Operating Voltage	110 to 240 VAC RMS
		Operating Current	1.5 A RMS
		Operating Frequency Range	50 to 60 Hz AC
Lithium-Ion Battery Pack (8-cell)	**Dimensions** (L x W x D)	4.95 x 3.46 x 0.80 in (12.5 x 8.8 x 2.0 cm)	
	Weight	0.96 lb (0.43 kg)	
	Energy	Voltage	14.8 V
		Amp-hour capacity	Minimum 3.7 Ah Typical 3.9 Ah
		Watt-hour capacity	Minimum 53.2 Ah Typical 56.1 Ah
	Temperature	Operating	32° to 108° F (0° to 42° C)
		Non-operating	32° to 140° F (0° to 60° C)
DVD/CD-RW Drive	**Center Hole Diameter**	15 mm	
	Disk Diameter	12 cm, 8 cm	
	Disk Thickness	1.2 mm	
	Track Pitch	1.6 µm	
	Access Times (typical reads, including settling)	Random CD	< 120 ms
		Full-Stroke CD	< 175 ms
	Disk Diameter	Random DVD	< 140 ms
	Disk Thickness	Full-Stroke DVD	< 225 ms
	Audio Output Level	0.7 – 0.9 Vrms	
	Cache Buffer	2 Mbytes (minimum)	
	Data Transfer Rate	CD-R (8X)	1200 KB/s

24.601

	(typical, including settling)		(150 KB/s at 1X CD rate)
		CD-RW (8X)	1200 KB/s (150 KB/s at 1X CD rate)
		CD-ROM (24X)	3600 KB/s (150 KB/s at 1X CD rate)
		DVD (8X)	10,800 KB/s (1352 KB/s at 1X DVD rate)
		Normal PIO Mode 4 (single burst)	16.6 MB/s
	Start-up Time	Single	< 7 seconds (typical)
		Multi-Session	< 30 seconds (typical)
	Stop Time	< 3 seconds (typical)	
DVD-ROM Drive	**Center Hole Diameter**	0.59 in (1.5 cm)	
	Disc Diameter	12 cm/8 cm	
	Disc Thickness	1.2 mm	
	Track Pitch	0.74 µm	
	Access Times (typical reads, including settling)	Random (typical)	< 125 ms DVD Media
		Full-Stroke (typical)	< 225 ms DVD Media
		Random (typical)	< 100 ms CD Media
		Full-Stroke (typical)	< 175 ms CD Media
	Cache Buffer	512 KB/s (minimum)	
	Data Transfer Rate (typical, including settling)	Max 24X CD	3600 KB/s (150 KB/s at 1X CD rate)
		Max 8X DVD	10,800 KB/s (1352 KB/s at 1X DVD rate)
	Start-up Time	< 12 seconds Typical	
	Stop Time	< 3 seconds Typical	
24X CD-ROM Drive	**Applicable Disk**	CD-ROM (Mode 1, 2 and 3), CD-XA ready (Mode 2, Form 1 and 2), CD-I ready (Mode 2, Form 1 and 2), CD-R (read only), CD Plus, Photo CD (Single and Multi-session), CD-Extra, Video CD, CD-WO (fixed packets only), CD-Bridge	
	Center Hole Diameter	0.59 in (15 mm)	
	Disk Diameter	12 cm, 8 cm	
	Disk Thickness	0.047 in (1.2 mm)	
	Track Pitch	1.6 µm	
	Access Times (typical reads, including settling)	Random	< 110 ms
		Full-Stroke	< 220 ms
	Audio Output Level	Line-out	0.7-0.9 Vrms
	Cache Buffer	128 KB	
	Data Transfer Rate	CD-ROM	3600 KB/s Maximum

149

24.600

	(typical, including settling)		
	Start-up Time	< 10 seconds	
	Stop Time	< 5 seconds	
802.11b MultiPort Module	**Form Factor**	Compaq "MultiPort"	
	Weight	0.22 lb/100 g (maximum)	
	Operating Temperature	Operating	14° to 149° F (–10° to 65° C)
	Storage Temperature	Non-operating	–40° to 176° F (–40° to 80° C)
	Humidity	Operating	10 to 90%
		Non-operating	5 to 95%
	Altitude	Operating	0 to 15,000 ft (4,572 m)
		Non-operating	0 to 40,000 ft (12,192 m)
	Plug and Play	USB 1.1 compliant	
		Microsoft Windows Plug and Play compliant	
	RF Network Standard	IEEE 802 Part 11b (802.11b)	
	Frequency Band	2,4000 to 2.4835 GHz	
		2,4465 to 2.4835 GHz (France)	
		2,4000 to 2,4697 GHz (Japan)	
	Number of Selectable Sub-channels	**Worldwide Certification**	
		United States (FCC)	11
		France (FR)	4
		Japan (JP)	14
		Other countries	13
	Data Rates	1, 2, 5.5, 11 Mbps	
	Antenna type	Internally integrated within module (with special polarization diversity)	
	WEP Security	64-bit encryption keys compliant to IEEE 802.11	
		128-bit encryption key compliant to IEEE 802.11	
		Ability to enter keys manually or via pass-phrase	
	Network Architecture Models	Ad-hoc (Peer to Peer)	
		Infrastructure (Access Points Required)	
	Modulation Technique	Direct Sequence Spread Spectrum: DBPSK, DQPSK, CCK	
	Receiver Sensitivity – Bit Error Rate (1E-5)	11 Mbps: -85 dBm	
		5.5 Mbps: -87 dBm	
		2 Mbps: -91 dBm	
		1 Mbps: -94 dBm	
	Maximum Receive Level	–4 dBm	
	Output Power (approximately)	18 dBM	
	Operating Voltage	5V power operation	
	Power Management	Keystroke Fn+F2 Power On/Off control	

250

Power Consumption	Transfer mode: < 600 mA, maximum	
	Receive mode: > 400 mA, maximum	
	Standby mode: > 1 mA, maximum	
Transmit Power	10 to 100mW It is preferable to have the user configurable output power to save battery life for laptop users or in high AP coverage areas	
Power Saving Option	802.11 Compliant Power Saving	
	Power Saving Mode selectable through the configuration utility	
	ACPI compliant power management	
Media Access Protocol	CSMA/CA (Collision Avoidance) with ACK	
OS Support	Microsoft Windows 2000	
	Microsoft Windows XP Home	
	Microsoft Windows XP Pro	
Protocols Supported	TCP/IP	
	IPX/SPX	
	UDP	
LED Activity	Flashing LED – AP Search Mode	
	Solid LED – On	
	LED Off – Power Off	

	Throughput	**Data Rate**	**Operating Distance**
Throughput, Data Rate and Operating Distance	> 4.5 Mbps	11 Mbps	• 1000 feet – Open sight • 100 feet – Closed space (Steel Space)
	> 2 Mbps	5.5 Mbps	• 1100 feet – Open sight • 200 feet – Closed space (Steel Space)
	> 700 Kbps	1 Mbps	• 1200 feet – Open sight • 300 feet – Closed space (Steel Space)

Bluetooth MultiPort Module	**Form Factor**	Compaq "MultiPort"	
	Bluetooth	1.1 Compliant	
	Dimensions	2.2 x 6.6 x 0.55 in (5.6 x 16.7 x 1.4 cm)	
	Weight	0.22 lb (100 g) (maximum)	
	Temperature	Operating	50° to 104° F (10° to 40° C)
		Non-operating	–4° to 140° F (–20° to 60° C)
	Humidity	Operating	10 to 90%
		Non-operating	5 to 95%
	Altitude	Operating	0 to 10,000 ft (3,048 m)

	Non-operating 0 to 30,000 ft (9,144 m)
Plug and Play	USB 1.1 compliant Microsoft Windows Plug and Play compliant
Frequency Band	2,4000 to 2.4835 GHz
Number of Available Channels	79 (1 MHz) available channels
Data Rates and throughput	1 Mbps Synchronous Connection Oriented links up to 3, 64 kbps, voice channels Asynchronous Connection Less links 723.2 kbps/57.6 kbps asymmetric or 433.9 kbps symmetric
Antenna type	Internally integrated within module (with special polarization diversity)
Range	328 ft/100 m
Profile Support	General Access Profile Service Discovery Application Profile Serial Port Profile Generic Object Exchange Profile File Transfer Profile Synchronization Profile Dial-Up Networking Profile LAN Access Profile Object Push Profile
Usage Models	Service Discovery (determine what Bluetooth devices are within range and support authorization) **Synchronization**: PDAs to PCs Portable to Desktop **File Transfer**: File and directory browsing and navigation on another Bluetooth device. File copying Object manipulation – including add, delete, create new folders etc. Wireless link to Corporate LAN using several Bluetooth devices sharing the same **Access Point**: Corporate email, network neighborhood, access to LAN applications, file transfer, ftp, Internet browsing, etc, using TCP/IP Wireless link to WAN thru cell phone GSM/SMS, PCS, PHS, DECT, RAM, ARDIS, CDPD, etc. Agnostic to WAN technology Send/receive SMS messages Wireless link to Printer Adhoc peer to peer networking (two computers) or Personal Area Networking (PAN) using NDIS (< 7 computers)

		Adhoc Bluetooth Pico-networking (point to multi-point) Object Push – Business card or appointment exchange
	Transmit Power	< 20 dBM (Bluetooth Class 1)
	Receive Sensitivity	Better than –70 dBM at 0.1 % raw bit error rate
	Link Topology	Point to Point, Multipoint Pico Nets up to 7 slaves
	Security	Full support of Bluetooth Security Provisions
	Network Architecture Models	Ad-hoc (Peer to Peer) Infrastructure (Access Points Required)
	Power Requirement	Peak < 1500 mW Average < 500 mW Standby < 250 mW
	Power Management	Microsoft Windows ACPI, and USB Bus Support Keystrokes Fn+F2 Power On/Off control Self configurable to optimize power conservation in all operating modes, including Standby, Hold, Park, and Sniff
	OS Support	Microsoft Windows 2000 Microsoft Windows XP Home Microsoft Windows XP Pro
	Protocols Supported	TCP/IP IPX/SPX UDP
	LED Activity	Solid Blue LED – On LED Off – Power Off
	Certifications	All necessary regulatory approvals for countries we support including: FCC (47 CFR) Part 15C, Section 15.247 & 15.249 ETS 300 328, ETS 300 826 Low Voltage Directive IEC950 UL, CSA, and CE Mark
Type III Mini PCI 56K (V.92) **Modem**	**Form Factor**	Mini-PCI Type III per Specification
	Power Management Support	APM Revision 1.2, ACPI, Compaq Power Management Extensions for Microsoft Windows NT®
	Approvals/Certifications	UL, CSA, NEMKO, CCIB, Industry Canada, FCC Part 68, CTR21, FCC Part 15 Class B, Canadian ICES-003 Class B, C.I.S.P.R.22, Australian ACA, CE Mark, Other Countries
	Data Mode Capabilities	V.92 (a-law, mu-law) K56flex (a-law, mu-law) V.8bis V.80 V44.bis, MNP5 (Compression) V42.bis, MNP5 (Compression) V.42 (LAPM, MNP2-4) (Error Correction)

		V.34 (file date: 10/96)
		Optional symbol rates:
		2800, 3429 Asymmetric Symbol rates
		Synchronous primary channel data signaling rates:
		3600, 31200 Automatic rate re-negotiation V.32bis V.32 V.23 V.22bis V.22 V.21 Bell 212A Bell 103J
	Fax Mode Capabilities	TIA-578-S (Class 1)
		T.30, T.4 (Group 3)
		V.17
		V.29
		V.27ter
		V.21 Channel 2
	Command Set	V.250 (Partial)
		TIA-602
		Identification: + GMI, + GMM, + GMR
		Port control: + IPR, + ICF, + IFC, + ILRR
		Modulation: + MS, + MR, + MA
		Error control: + ES, + ER, + EB, + ESR, + ETBM
		Data compression: + DS, + DR
		V.251
Integrated 10/100 NIC	**NIC Device Driver Name**	RealTek (RTL 8139CL+)
	Data Link Layers	IEEE 802.2 LLC
		SNAP
	Ethernet Features	10 Mbps Ethernet: IEEE 802.3 standard 10BASE-T
		100 Mbps Ethernet: IEEE 802.3u standard 100BASE-TX
		Full Duplex at 10 and 100Mbps
		Auto-Negotiation
		Wake on LAN from standby
		Boot on LAN from OFF
		Lower Power State on Link Loss
	Software support	IBM LAN Server Version 1.2, 1.3, 2.0, 4.0
		Microsoft NT 3.51, NT 4.0. Microsoft Windows 2000
		Novell Netware 3.1x, 4.x, 5.x
	Protocol support	TCP/IP

Novell IPX/SPX and Microsoft compatible
Novel IPX ODI
Microsoft NetBEUI
IBM DLC

HP recommends Microsoft® Windows® XP Professional for Mobile Computing

---

DA-11455 - U.S. - Version 8 - June 10, 2003

24.594

QuickSpecs

HP USB and PS/2 Easy Access Keyboards

Models

Compaq USB Easy Access Keyboard (carbon/silver)
DC168A
HP USB Easy Access Keyboard (carbonite/silver)
DC168B
Compaq PS/2 Easy Access Keyboard BG1650 (gray)
DC636A
HP PS/2 Easy Access Keyboard BG1650 (gray)
DC636B
Compaq PS/2 Easy Access keyboard (carbon/silver)
DC167A
HP PS/2 Easy Access keyboard (carbonite/silver)
DC167B

Overview

The HP-branded Easy Access Keyboards are a family of keyboards based upon the same form factor and keystroke design but offering a variety of connection and color differences. The 267146-xx8 and 267145-xx8 are identical, with the exception of connection technology. The 267145-xx8 is PS/2 (legacy communication protocol) and the 267146-xx8 is the USB more recent plug-and-play communication protocol. The 267145-xx4 is the same PS/2 variant as the 267145-xx8 but complies with BG1650 ergonomic and color specification. Both USB and PS/2 are available in 104, 105, 106, 107 and 109-key forms to comply with 36 local language layout requirements. The BG1650 variant has 105 keys and is offered in 8 local language layouts (International, Belgian, Danish, French, German, Italian, Swedish, Swiss).

HP Easy Access Keyboards facilitate frequent use of the Internet by providing easy, immediate access to Web-based information at the touch of a button. Users who repeatedly access Internet or intranet web sites will appreciate the expanded functionality and ease of use of these keyboards. Through the client-based Easy Access Keyboard software utility, they can customize the eight pre-programmed buttons to gain instant access to Internet addresses, applications, or files. HP Easy Access keyboards work in conjunction with server-based Redirector software, allowing customers to customize and change Intranet landing sites without affecting firmware. The Redirector server is maintained and managed by PSG Engineering in Houston. The Softkey icon insert that sits beneath the plastic clear lens can be customized for unique icon specification. Contact Wetmore Printing, Houston for details on icon customization and replacement.

Key Benefits

- Saves time and effort by directing users instantly to targeted Internet destinations
- Allows customized programming of buttons to launch user-specified applications
- Features pre-programmed buttons for easy access to useful business web sites
- Provides easy, immediate access to critical information at the touch of a button
- Directs users instantly to targeted Internet destinations
- Increases productivity by reducing time spent typing Web addresses
- Permits users to customize buttons to suit individual requirements
- Facilitates instant access to Internet addresses, applications, or files via eight programmable buttons
- Fits the needs and capabilities of the average user as well as those of the IT professional

Compatibility

Compaq USB and PS/2 Easy Access Keyboards (carbon/silver) are compatible with Compaq Evo

D300 and D500 Series PCs (except for the PS/2 Easy Access Keyboard which is not compatible with the Compaq Evo D510 e-pc) and HP Workstations xw4000, xw5000, xw6000 and xw8000.
The Compaq PS/2Easy Access Keyboard BG1650 (DC636A) is compatible with Compaq Evo D310 and D500 Series PCs (except the Compaq Evo D510 e-pc)
HP USB and PS/2 Easy Access Keyboards (carbonite/silver) are compatible with the HP Compaq Business Desktop d220, d230, d330 and d530 Series PCs and the HP Business Desktop d325 Microtower and HP Workstations.
The HP PS/2Easy Access Keyboard BG1650 (DC636B) is compatible with HP Compaq Business Desktop d330 and d530 Series PCs and the HP Business Desktop d325 Microtower.

Service and Support

HP Easy Access Keyboards have a One-year Limited Warranty or the remainder of the warranty of the HP product in which it is installed. Technical support is available seven days a week, 24 hours a day by phone, as well as in online support forums. Certain restrictions and exclusions apply.

Specifications

USB Easy Access Keyboard

Physical characteristics	**Keys**	104, 105, 106, 107, 109 layout (depending upon country) plus eight programmable keys for Internet, shortcuts, or multimedia
	Dimensions (L x W x H)	18.0 x 6.3 x 1.3 in (45.8 x 16.1 x 3.3 cm)
	Weight	2 lb (0.9 kg) minimum
Electrical	**Operating voltage**	+ 5VDC +/- 5%
	Power consumption	50-mA maximum (with three LEDs ON)
	System interface	USB Type A plug connector
	ESD	CE level 4, 15-kV air discharge
	EMI - RFI	Conforms to FCC rules for a Class B computing device
	Microsoft PC 99 - 2001	Functionally compliant
Mechanical	**Languages**	30+ available
	Keycaps	Low-profile design
	Switch actuation	55-g nominal peak force with tactile feedback
	Switch life	20 million keystrokes (using Hasco modified tester)
	Switch type	Contamination-resistant membrane
	Key-leveling mechanisms	For all double-wide and greater-length keys
	Cable length	6 ft (1.8 m)
	Microsoft PC 99 - 2001	Mechanically compliant
	Acoustics	43-dBA maximum sound pressure level
Environmental	**Operating temperature**	50° to 122° F (10° to 50° C)
	Non-operating temperature	–22° to 140° F (–30° to 60° C)
	Operating humidity	10% to 90% (non-condensing at ambient)

	Non-operating humidity	20% to 80% (non-condensing at ambient)
	Operating shock	40 g, six surfaces
	Non-operating shock	80 g, six surfaces
	Operating vibration	2-g peak acceleration
	Non-operating vibration	4-g peak acceleration
	Drop (out of box)	26 in (66 cm) on carpet, six-drop sequence
	Drop (in box)	42 in (107 cm) on concrete, 16-drop sequence
Operating system support	Windows 2000, and XP	
Approvals	CE-Mark, UL, CSA, FCC, CE Mark, TUV, TUV GS, VCCI, BSMI, C-Tick, MIC	
Ergonomic compliance	ANSI HFS 100, ISO 9241-4, and TUVGS	
Kit contents	Keyboard, keyboard software media, installation guide, warranty card, safety and comfort guide	

PS/2 Easy Access Keyboard BG1650 (gray)

Physical characteristics	**Keys**	104, 105, 106, 107, 109 layout (depending upon country) plus eight programmable keys for Internet, shortcuts, or multimedia
	Dimensions (L x W x H)	18.0 x 6.3 x 1.3 in (45.8 x 16.1 x 3.3 cm)
	Weight	2 lb (0.9 kg) minimum
Electrical	**Operating voltage**	+ 5VDC +/- 5%
	Power consumption	50-mA maximum (with three LEDs ON)
	System interface	PS/2 6-pin mini din connector
	ESD	CE level 4, 15-kV air discharge
	EMI - RFI	Conforms to FCC rules for a Class B computing device
	Microsoft PC 99 - 2001	Functionally compliant
Mechanical	**Languages**	30+ available
	Keycaps	Low-profile design
	Switch actuation	55-g nominal peak force with tactile feedback
	Switch life	20 million keystrokes (using Hasco modified tester)
	Switch type	Contamination-resistant membrane
	Key-leveling mechanisms	For all double-wide and greater-length keys
	Cable length	6 ft (1.8 m)
	Microsoft PC 99 - 2001	Mechanically compliant

24.591

	Acoustics	43-dBA maximum sound pressure level
Environmental	**Operating temperature**	50° to 122° F (10° to 50° C)
	Non-operating temperature	–22° to 140° F (–30° to 60° C)
	Operating humidity	10% to 90% (non-condensing at ambient)
	Non-operating humidity	20% to 80% (non-condensing at ambient)
	Operating shock	40 g, six surfaces
	Non-operating shock	80 g, six surfaces
	Operating vibration	2-g peak acceleration
	Non-operating vibration	4-g peak acceleration
	Drop (out of box)	26 in (66 cm) on carpet, six-drop sequence
	Drop (in box)	42 in (107 cm) on concrete, 16-drop sequence

Operating system support	Microsoft® Windows 2000, and XP
Approvals	CE-Mark, UL, CSA, FCC, CE Mark, TUV, TUV GS, VCCI, BSMI, C-Tick, MIC
Ergonomic compliance	ANSI HFS 100, ISO 9241-4, and TUVGS
Kit contents	Keyboard, keyboard software media, installation guide, warranty card, safety and comfort guide

PS/2 Easy Access keyboard

Physical characteristics	**Keys**	104, 105, 106, 107, 109 layout (depending upon country) plus eight programmable keys for Internet, shortcuts, or multimedia
	Dimensions (L x W x H)	18.0 x 6.3 x 1.3 in (45.8 x 16.1 x 3.3 cm)
	Weight	2 lb (0.9 kg) minimum
Electrical	**Operating voltage**	+ 5VDC +/- 5%
	Power consumption	50-mA maximum (with three LEDs ON)
	System interface	PS/2 6-pin mini din connector
	ESD	CE level 4, 15-kV air discharge
	EMI - RFI	Conforms to FCC rules for a Class B computing device
	Microsoft PC 99 - 2001	Functionally compliant
Mechanical	**Languages**	30+ available
	Keycaps	Low-profile design
	Switch actuation	55-g nominal peak force with tactile feedback
	Switch life	20 million keystrokes (using Hasco modified tester)

	Switch type	Contamination-resistant membrane
	Key-leveling mechanisms	For all double-wide and greater-length keys
	Cable length	6 ft (1.8 m)
	Microsoft PC 99 - 2001	Mechanically compliant
	Acoustics	43-dBA maximum sound pressure level
Environmental	**Operating temperature**	50° to 122° F (10° to 50° C)
	Non-operating temperature	–22° to 140° F (–30° to 60° C)
	Operating humidity	10% to 90% (non-condensing at ambient)
	Non-operating humidity	20% to 80% (non-condensing at ambient)
	Operating shock	40 g, six surfaces
	Non-operating shock	80 g, six surfaces
	Operating vibration	2-g peak acceleration
	Non-operating vibration	4-g peak acceleration
	Drop (out of box)	26 in (66 cm) on carpet, six-drop sequence
	Drop (in box)	42 in (107 cm) on concrete, 16-drop sequence
Operating system support	Microsoft Windows 2000, and XP	
Approvals	CE-Mark, UL, CSA, FCC, CE Mark, TUV, TUV GS, VCCI, BSMI, C-Tick, MIC	
Ergonomic compliance	ANSI HFS 100, ISO 9241-4, and TUVGS	
Kit contents	Keyboard, keyboard software media, installation guide, warranty card, safety and comfort guide	

HP recommends Microsoft® Windows® XP Professional for Business

DA-11357 - U.S. - Version 4 - June 10, 2003

RELAÇÃO DE CENTRAIS DE ATENDIMENTO

Estados: Selecione um Estado abaixo.

REGIÃO DE ATUAÇÃO	UNIDADE	CNPJ	INSCRIÇÃO ESTADUAL	INSCRIÇÃO MUNICIPAL	FAX	TELEFONE
Brasília e algumas cidades de MG	CAT-BRA	42.318.949/0013-18	07.322.007/002-03	025.815-1	(61) 349-3930 (61) 349-1913	(61) 349-2400

RESPONSÁVEL TÉCNICO	DISPONIBILIDADE 7X24	ENDEREÇO
Marcia Araújo	SIM	SEUPN, Quadra 511 Bloco B, nr. 57, Lote 02 - 3o andar - Ed. Bittar III - Asa Norte - Brasília - DF - 70550-527

855.170

1062

RELAÇÃO DE CENTRAIS DE ATENDIMENTO

Estados: Selecione um Estado abaixo.

REGIÃO DE ATUAÇÃO	UNIDADE	CNPJ	INSCRIÇÃO ESTADUAL	INSCRIÇÃO MUNICIPAL	FAX	TELEFONE
SP-capital, Mogi das Cruzes, ABC e Baixada Santista	CAT-SPO	42.318.949/0004-27	109.895.039.119	8.363.027-9	(11) 283-5322 (11) 287-1740	(11) 251-3311

RESPONSÁVEL TÉCNICO	DISPONIBILIDADE 7X24	ENDEREÇO
Laerte Candido	SIM	Alameda Santos, 1000, cj.71 e 72 - Cerqueira Cesar - São Paulo - SP - 01418-100

24.587

ANEXO SOFTWARE

COBRA Tecnologia S.A.
Estrada dos Bandeirantes 7966
CEP 22783-110 Rio de Janeiro RJ
Tel. 21 442-8800
www.cobra.com.br

Oracle9*i*

Release Notes

Release 2 (9.2.0.1.0) for HP 9000 Series HP-UX (64-bit)

June 2002

Part No. A97350-02

This document accompanies Oracle9*i* release 2 (9.2.0.1.0) for HP 9000 Series HP-UX (64-bit). Its contents supplement or supersede information in the installation guide for this release, or in the Oracle9*i* documentation library.

Topics:

- System Requirements
- Documentation
- Installation Issues
- Product-Related Issues
- Post-Installation Issues
- Known Bugs

System Requirements

Except as noted here, system requirements are in the installation guide for this release, and are current as of the release date.

Hard Disk Space Requirements

The space requirements listed on the Available Products window apply to installations that include a database. If you select the Software Only configuration type, then you will require 3 GB.

Additional Software Patch Requirements

If you are installing Oracle Real Application Clusters on HP-UX 11.0, and if you are using the HMP protocol, then you must download the following patch from HP in addition to the patches listed in the installation guide.

- PHNE_26551

If you are installing Oracle Real Application Clusters on HP-UX version 11*i* (11.11), and if you are using the HMP protocol, then you must download the following patch from HP in addition to the patches listed in the installation guide.

- PHNE_27114

If you are installing HP-UX version 11*i* (11.11), then you must download the following OS patches:

- GOLDQPK11i (includes both GOLDAPPS11i and GOLDBASE11i)
- PHKL_25506
- PHSS_26263
- PHSS_24638
- JDK 1.3.1.02

If you are using ServiceGuard OPS Edition version 11.13 for HP-UX lli, then you must install the following patch:

- PHSS_26674

> **Note:** In the near future, *ServiceGuard OPS Edition* will be replaced with *ServiceGuard Extension for RAC*.

Updated Requirements

Oracle Corporation updates these release notes online at the following site:

`http://docs.oracle.com`

If you need assistance with navigating the Oracle documentation site, refer to the following site:

`http://docs.oracle.com/instructions.html`

Refer also to the Certify Web Pages on Oracle*MetaLink*, which provide certified configuration information for Oracle and non-Oracle products. To access Certify:

1. Register or log in to Oracle*MetaLink* at the following Web address:

   `http://metalink.oracle.com`

2. Select Product Lifecycle from the Oracle*Metalink* navigation bar.
3. Select Certifications in the Product Lifecycle window navigation bar.

Oracle Universal Installer Version Update

Oracle9*i* release 2 (9.2.0.1.0), which is provided with the release, uses Oracle Universal Installer 2.2.0.12.0. This version number supersedes the version listed in the installation guide.

Documentation

Additional product `README` files are located in their respective product directories under the `$ORACLE_HOME` directory and in the `$ORACLE_HOME/relnotes` directory.

Documentation Errata

The following is a list of errors in the documentation for this release.

PL/SQL Gateway

In Appendix A, "Oracle9*i* Components," in *Oracle9i Installation Guide Release 2 (9.2.0.1.0) for UNIX Systems*, PL/SQL Gateway is listed as a supported product. It has been desupported for this release.

Pre-Installation Requirements

Under "Random Access Memory" on page 2-3 in Chapter 2, "Pre-Installation Requirements, in *Oracle9i Installation Guide Release 2 (9.2.0.1.0) for UNIX Systems*, the Linux and HP commands are reversed. The correct commands are the following:

Linux

```
$ grep MemTotal /proc/meminfo
```

HP

```
$ /usr/sbin/dmesg | grep "Physical:"
```

Installation Issues

This section provides information about the following topics:

- 32-bit O/S Support
- Multiple CD-ROM Installation
- runInstaller Script
- Installing Databases with Database Configuration Assistant
- Database Migration

32-bit O/S Support

Do not run Oracle9*i* on a 32-bit operating system. Oracle9*i* release 2 (9.2.0.1.0) is offered in a 64-bit version only. If you try to run any 64-bit executables on a 32-bit operating system, then they will fail. If you run Oracle9*i* release 2 (9.2.0.1.0) on a 32-bit system, then you will see the following error message:

```
./oracle: Exec format error. Wrong Architecture.
```

Multiple CD-ROM Installation

During the installation of Oracle9*i* release 2 (9.2.0.1.0), you will be prompted to insert additional CD-ROMs from the set that make up Oracle9*i* release 2 (9.2.0.1.0). When prompted to mount the next CD-ROM, use the following procedure:

1. On the window where you have started the Installer, press Enter to go to the UNIX prompt, and then change the directory to your system's root directory. Log in as the `root` user by using the following commands:

   ```
   $ cd /
   $ su root
   ```

2. Unmount and remove the CD-ROM from the CD-ROM drive with the following command:

   ```
   # /usr/sbin/pfs_umount/SD_CDROM
   ```

3. Insert the required CD-ROM into the CD-ROM drive and mount it by using the following command:

   ```
   # /usr/sbin/pfs_mount/SD_CDROM
   ```

4. Click OK to continue.

runInstaller Script

Because it is necessary to insert and eject more than one CD-ROM during installation, you must not launch Oracle Universal Installer by running the `runInstaller` script from a shell where the current working directory is the CD-ROM mount point, or by clicking on the script in the *File Manager* window. In an X Window environment, it is possible to launch the Installer this way, but then the installation will fail because you will not be able to eject a software CD-ROM until you end the installation session.

Installing Databases with Database Configuration Assistant

Review the following information before running Database Configuration Assistant.

SYS and SYSTEM Password Change Requirement

If you use Database Configuration Assistant to create a database, be aware that you will be required to change the SYS and SYSTEM passwords at the end of the configuration process. This is a new security procedure designed to protect access to your data.

Database Migration

If you are upgrading from release 8.0.6 to release 9.2.0.1.0 and you have Oracle *inter*Media installed on your system, then you cannot use Database Migration Assistant. You must migrate the database manually. For information on manual database migration, refer to *Oracle9i Database Migration Release 2 (9.2)*.

Installing with Response Files

For installation with a response file, the path to the response file must be the full path on the system. The Oracle Universal Installer does not handle relative paths properly.

Unzip Utility for Downloading and Installing Oracle Patches

An unzip utility is provided with Oracle9*i* release 2 (9.2.0.1.0) for uncompressing Oracle patches downloaded from Oracle*MetaLink*. The utility is located in the following directory:

```
$ORACLE_HOME/bin/
```

Product-Related Issues

This section provides information on the following topics:

- Character Sets
- Demo Schema
- Java Database Connectivity Driver
- Oracle Advanced Security
- Oracle Internet Directory (OID)
- Oracle Real Application Clusters

Character Sets

The following section provides information on restrictions and updates to character sets.

Oracle9*i* NCHAR Datatypes

In Oracle9*i* release 2 (9.2.0.1.0), the SQL NCHAR datatypes are limited to the Unicode character set encoding (UTF8 and AL16UTF16). Alternative character sets such as the fixed-width Asian character set JA16SJISFIXED in Oracle8*i* are no longer supported.

To migrate existing NCHAR, NVARCHAR, and NCLOB columns, export and import NCHAR columns, complete the following steps:

1. Export all SQL NCHAR columns from Oracle8*i*.
2. Drop the SQL NCHAR columns.
3. Migrate the database to Oracle9*i*.
4. Import the SQL NCHAR columns in to Oracle9*i*.

AL24UTFFSS Character Set

Oracle9*i* release 2 (9.2.0.1.0) does not support the Unicode character set AL24UTFFSS introduced in Oracle7. This character set was based on the Unicode standard 1.1, which is now obsolete.

Oracle9*i* release 2 (9.2.0.1.0) supports the Unicode database character sets AL32UTF8 and UTF8. These database character sets include the Unicode enhancements based on the Unicode standard 3.0.

To migrate the existing AL24UTFFSS database, upgrade your database character set to UTF8 before upgrading to Oracle9*i*. Oracle Corporation recommends that you use the Character Set Scanner for data analysis before attempting to migrate your existing database character set.

Character Set Scanner

Set the LD_LIBRARY_PATH variable to include the `$ORACLE_HOME/lib` directory before running the Character Set Scanner (csscan) from the `$ORACLE_HOME` directory. If you do not correctly set the LD_LIBRARY_PATH variable, then the csscan utility will fail.

Demo Schema

If you select a multibyte character set or UTF as the national character set in Oracle9*i* release 2 (9.2.0.1.0), then you must recreate the demo schema and the database installation.

For more information on creating schemas, schema dependencies and requirements, refer to the `readme.txt` file in the `$ORACLE_HOME/demo/schema` directory.

Java Database Connectivity Driver

The default behavior for the `ResultSet::getXXXStream()` has been modified to comply with the Java Database Connectivity (JDBC) specification so that the APIs return null values for database null `LONG/LONG RAW` values.

For Oracle8*i* release 8.1.*x* JDBC drivers, the default behavior was to return an empty stream for database null values. The Java property `jdbc.backward_compatible_to_8.1.7` allows the system to use the earlier JDBC default behavior when using the Oracle9*i* drivers and applies to Oracle9*i* JDBC Thin and OCI drivers.

For example, if the Java property is set at the virtual machine runtime, the following command will cause the Oracle9*i* JDBC drivers to return empty streams from calls to `ResultSet::getXXXStream()`:

```
java -Djdbc.backward_compatible_to_8.1.7 myJavaProgram
```

Oracle Advanced Security

If you install `jsse.jar` and `jcert.jar` as extensions (located in `$JAVA_HOME/jre/lib/ext`), then you must also install `jssl-1_1.jar` in the same directory.

Oracle Internet Directory (OID)

Review the following information if you intend to install Oracle Internet Directory (OID).

Starting Up OID Server

By default, the OID server is started on port 389. If this port is unavailable, then OID server is started on a different port, which is logged in the following file:

```
$ORACLE_HOME/ldap/install/oidca.out
```

Custom Installation and Global Database Name

When performing a custom Oracle Internet Directory installation, do not change the global database name or the Oracle SID.

Upgrade from Enterprise Edition Oracle9*i* or Oracle8*i*

If you have installed in the same ORACLE_HOME either Oracle Internet Directory release 3.0.1.*x* and the complete release of Oracle9*i* (9.0.1) Enterprise Edition, or Oracle Internet Directory 2.1.1.*x* and the complete release of Oracle8*i* (8.1.7) Enterprise Edition, then you must first upgrade Oracle Internet Directory to the release 9.2.0.*x.x* version, and then upgrade as a separate step either Oracle9*i* Enterprise Edition Release 1 (9.0.1) or Oracle8*i* release 3 (8.1.7) to Oracle9*i* Enterprise Edition Release 2 (9.2.0.*x.x*).

> **See Also:** *Oracle Internet Directory README* for more information on Oracle Internet Directory utilities, and necessary pre-upgrade and post-upgrade tasks.

Oracle Real Application Clusters

Review the following section if you will install Oracle Real Application Clusters.

Restrictions for Installing Real Application Clusters

The following restrictions apply for this release:

- The Cluster Manager implementation may not be able to handle 32-bit and 64-bit clients concurrently. This will prevent 32-bit and 64-bit Oracle Real Application Clusters executables from being used at the same time within the same cluster domain.

  If a database is not set up with the Oracle Real Application Clusters option, then this restriction does not apply to the Oracle executables.

- If you are installing Oracle9*i* release 2 (9.2.0.1.0) Real Applications Clusters on a cluster that already contains an ORACLE_HOME for a previous release of Real Application Clusters, then you must run the Oracle Universal Installer from the cluster node with the oraInventory installation registry. Doing this ensures that product installation inventories are synchronized on the nodes with information about existing ORACLE_HOME directories.

Real Application Clusters Custom Installation Requirement

If you plan to create an Oracle Enterprise Manager repository in an existing database, and you plan to use the DRSYS tablespace for the repository, then ensure that the DRSYS tablespace raw device data file has an additional 50 MB of free space. This is in addition to the 250 MB size documented for this raw device.

Real Application Clusters and Database Upgrade Assistant

If you use Database Upgrade Assistant to upgrade an earlier Oracle database version (the "source" database) to Oracle9*i* release 2 (9.2.0.1.0) (the "target" database), then the upgraded database will always use the server parameter file SPFILE by default to store `init.ora` file parameters. If the source database also uses SPFILE (either a cluster filesystem file or a shared raw device), then the upgraded target database also uses the same SPFILE.

If the source database does not use an SPFILE, then the target database uses a default server parameter file, `spfile.ora`, which is located in the `$ORACLE_HOME/dbs/` directory.

If your platform does not support a cluster file system, then you must move the SPFILE to a shared raw device, using the following procedure:

1. Create an SPFILE with the following commands:

```
$ sqlplus "/ as sysdba"
SQL> create pfile='?/dbs/initdbname.ora' from
spfile='?/dbs/spfile.ora';
SQL> create spfile='/dev/oracle_vg/dbname_spfile' from
pfile='?/dbs/initdbname.ora';
SQL> exit;
```

   where *dbname* is the name of your cluster database.

2. Go to the `$ORACLE_HOME/dbs` directory using the following command:

```
$ cd $ORACLE_HOME/dbs
```

3. Create an `$ORACLE_HOME/dbs/initsid.ora` file, where *sid* is the system identifier of the instance on the node. The `initsid.ora` file must contain the following line:

```
SPFILE='/dev/oracle_vg/dbname_spfile'
```

4. Copy the `initsid.ora` file to the remote nodes on which the cluster database has an instance with the following commands:

```
$ rcp initsid.ora nodex:$ORACLE_HOME/dbs/initsidx.ora
```

   where *sidx* is the system identifier of the instance on node *x*. Repeat the preceding `rcp` command for each member node of the cluster database.

5. Restart the cluster database with the following command syntax:

```
$ srvctl stop database -d dbname
$ srvctl start database -d dbname
```

Real Application Clusters and Database Configuration Assistant

The following section provides information on using Database Configuration Assistant (DBCA) to create a Real Application Clusters database.

Placing Datafiles On a Shared Non-OFA Cluster Configuration

If your ORACLE_HOME directory is not on a shared cluster filesystem partition, but you want to place datafiles, controlfiles, redo log files, or other database files on a shared cluster filesystem partition, then invoke DBCA using the following syntax to create the cluster database:

```
$ dbca -datafileDestination pathname
```

where *pathname* is the location where you want files to be placed.

For example, to place datafiles in the path `/ora/oradata`, give the following command:

```
$ dbca -datafileDestination /ora/oradata
```

Note: For optimal performance and data security, Oracle Corporation recommends that you configure your database in accordance with the Optimal Flexible Architecture (OFA) standard. For more information on OFA, refer to *Oracle9i Administrator's Reference for UNIX Systems*.

Real Application Clusters Instance Management

After you have created a cluster database using DBCA, SYSDBA privileges are revoked for all users. As SYSDBA, you must grant SYSDBA privileges explicitly to the database user account that you plan to use for adding or deleting an instance to or from the cluster database.

For example, to grant SYSDBA privileges to the administrative user SYS, issue the following commands:

```
$ sqlplus "/ as sysdba"
SQL> grant sysdba to sys;
SQL> exit;
```

Oracle Real Application Clusters and Upgrading from Oracle8*i*

If you are upgrading from Oracle8*i*, then set the `instance_number` initialization parameter in the `init.ora` file for all instances.

Oracle Real Application Clusters and HyperMessaging Protocol (HMP)

Complete the following three tasks prior to using HMP:

Ensure HF Software is Installed and Verified Ensure that you have the HyperFabric software installed, and verify that it exists. The HF software product ID number is B6257AA. Verify that it exists with the following command:

```
swlist | grep -i B6257AA
```

Configure HyperFabric Patch Use the following command to verify that the HyperFabric patch is configured properly before installing Oracle9*i*:

```
/opt/clic/bin/clic_stat
```

If the HyperFabric patch is configured properly, then the response to this command will list all nodes in the cluster. If cluster members are missing, then they will not appear in the response.

Note: The Hyper Messaging Protocol is not supported on V-class HP systems.

Tune HMP parameters Oracle Corporation recommends that you review parameters and tune them according to HP guidelines for optimal HMP performance. A list of HMP-tunable parameters can be found in the following file:

```
/opt/clic/lib/skgxp/skclic.conf
```

To enable Oracle to use HMP and to relink the Oracle binary with HMP, complete the following steps:

1. Set up your environment on all nodes
2. Shut down the database
3. Enter the following commands on all nodes:

```
$ cd $ORACLE_HOME/rdbms/ub
$ make -F ins_rdbms.mk ipc_hms ioracle
```

Platform-Specific Product Information

The following product information in this section supersedes the information in the installation guide for Oracle9*i* release 2 (9.2.0.1.0) on HP-UX.

- Precompiler Options:

  - Pro*COBOL (32-bit and 64-bit) are supported.
  - Pro*FORTRAN (32-bit and 64-bit) are supported.
  - SQL Module for Ada is not supported.
- Oracle Advanced Security:
  - Radius challenge response authentication is not supported.
  - CyberSafe is not supported.
  - DCE Integration is not supported.
- JDBC/OCI Interfaces:
  - Oracle JDBC Thin Driver for JDK 1.4 is not supported.
  - Oracle JDBC/OCI Driver for JDK 1.4 is not supported.

Post-Installation Issues

This section presents issues that can occur during post-installation:

Control File Size Limits

In addition to the database, a number of other Oracle features use control files to record metadata. The maximum size of control files is limited by the size of the minimum data block size that your operating system permits. On HP-UX, the minimum data block size is 2048 bytes, and the maximum size of control files is 20000 database blocks.

Support for 32-bit Client Applications

Oracle9*i* (64-bit) provides support for both 32-bit clients as well as 64-bit clients. By default, all demos and clients provided with this release link and run in 64-bit mode. You can, however, build 32-bit and 64-bit clients in the same `$ORACLE_HOME`.

The following combinations will run and link successfully in Oracle9*i* (64-bit):

- 32-bit applications against a 64-bit Oracle Server
- 64-bit applications against a 64-bit Oracle Server

The 64-bit client shared library is:

```
$ORACLE_HOME/lib/libclntsh.sl
```

The 32-bit client shared library is:

```
$ORACLE_HOME/lib32/libclntsh.sl
```

Building 32-bit Pro*C Customer Applications

Both 32-bit and 64-bit customer applications are supported in this release. Refer to the following files for further information:

```
$ORACLE_HOME/precomp/demo/demo_proc.mk
$ORACLE_HOME/precomp/demo/demo_proc32.mk
```

Building 32-bit OCI Customer Applications

Both 32-bit and 64-bit Oracle Call Interface (OCI) customer applications are supported in this release. Refer to the following file for further information:

```
$ORACLE_HOME/rdbms/demo/demo_rdbms.mk
```

32-bit Files and Directories

In Oracle9*i* (64-bit) for HP-UX (64-bit), the following directories contain 32-bit executables and libraries:

- `$ORACLE_HOME/lib32`
- `$ORACLE_HOME/rdbms/lib32`
- `$ORACLE_HOME/hs/lib32`
- `$ORACLE_HOME/network/lib32`
- `$ORACLE_HOME/precomp/lib32`

How to Determine Whether Segments or Tablespaces are Using Compression

The following section provides additional information about database management.

Segments and Compression Settings

To find out which database segments are using compression, log in to the database as the user SYS, and create the view `all_segs` with the following create or replace view statement:

```
SQL> create or replace view all_segs
     (owner, segment_name,
       partition_name, spare1
as
select u.name, o.name, o.subname, s.spare1
from sys.user$ u, sys.obj$ o, sys.ts$ ts, sys.sys_objects so,
```

```
      sys.seg$ s, sys.file$ f
 where s.file# = so.header_file
    and s.block# = so.header_block
    and s.ts# = so.ts_number
    and s.ts# = ts.ts#
    and s.ts# = so.object_id
    and o.owner# = u.user#
    and s.type# = so.object_type_id
    and s.ts# = f.ts#
    and s.file# = f.relfile#
union all
select u.name, un.name, NULLL, NULL
from sys.user$ u, sys.ts$ ts, sys.undo $ un, sys.seg$ s,
     sys.file$ f
where s.file# = un.file#
   and s.block# = un.block
   and s.ts# = un.ts#
   and s.ts# = ts.ts#
   and s.user# = u.user#
   and s.type# in (1, 10)
   and un.status$ != 1
   and un.ts# = f.ts#
   and un.file# = f.relfile#
union all
select u.name, to_char(f.file#)|| '.' || to_char(s.block#), NULL, NULL
from sys.user$ u, sys.ts$ ts, sys.seg$ s, sys.file$ f
where s.ts# = ts.ts#
   and s.user# = u.user#
   and s.type# not in (1, 5, 6, 8, 10)
   and s.ts# = f.ts#
   and s.file# = f.relfile#
/
```

After creating this view, you can issue queries against the view to find out whether a segment currently is compressed, as illustrated in the following examples:

- To determine if a segment is currently compressed, apply the following predicate in a query to the column `spare1`:

  ```
  bitand(spare1, 2048) > 0
  ```

  For example, to see if segments currently are compressed, issue a statement similar to the following:

  ```
  SQL> select * from all_segs where bitand(spare1,2048) > 0;
  ```

- To determine if a segment contains any compressed blocks, apply the following predicate in a query:

  ```
  bitand(spare1, 4096) > 0
  ```

For example, to see which segments contain any compressed blocks, issue a statement similar to the following:

```
SQL> select * from all_segs where bitand(spare1, 4096) > 0;
```

Tablespaces and Compression Settings

When you want to determine compression settings on a table space, log in as SYS, and create the view `compression_ts` with the following create or replace view statement:

```
SQL> create or replace view compression_ts (tablespace_name, flags) as
select ts.name, ts.flags from
sys.ts$ ts where ts.online$ !=3;
```

After creating this view, you can issue queries against it to find out the compression state of tablespaces, such as determining if a tablespace is currently set as DEFAULT COMPRESS, or DEFAULT NOCOMPRESS, as illustrated in the following examples:

- To determine if a tablespace is currently set as DEFAULT COMPRESS, use the following predicate:

  ```
  bitand(flags, 64) > 0
  ```

  For example, to see which tablespaces are currently DEFAULT COMPRESS, issue a statement similar to the following:

  ```
  SQL> select * from compression_ts where bitand(flags, 64) > 0
  ```

- To determine if a tablespace is currently set as DEFAULT NOCOMPRESS, use the following predicate:

  ```
  bitand(flags, 64) == 0
  ```

  For example, to see which tablespaces are currently DEFAULT NOCOMPRESS, issue a statement similar to the following:

  ```
  select * from compression_ts where bitand(flags, 64) == 0;
  ```

Known Bugs

The following is a list of known bugs that affect Oracle9*i* release 2 (9.2.0.1.0):

Error in JSP/Servlet Script

There is a path error in the `$ORACLE_HOME/bin/ojspc script`. This path error causes the script to fail. To correct this error:

1. Open the script
2. Find `$ORACLE_HOME/jsp/lib/servlet.jar`
3. Correct it to read `$ORACLE_HOME/lib/servlet.jar`
4. Save the script

Error Installing OLAP CWMLITE Tablespace

During installation, if you select Online Analytic Processing (OLAP) services, perform multiple installations on the same system, and create new databases during these installations, then CWMLite may have an invalid OLAP CWMLITE tablespace registry. Oracle Corporation has assigned bug identification number 2359208 to track this problem.

To work around this problem, use the following procedure after you have completed installation:

1. Ensure that the database and the listener are running.
2. Using the following command, start SQL*Plus as the administrative user SYS:

   ```
   sqlplus "/ as sysdba"
   ```

3. Using the following command, enable the display of text within the PL/SQL block:

   ```
   SQL> set serveroutput on;
   ```

4. Using the following command, verify whether the OLAP CWMLITE tablespace is valid:

   ```
   SQL> execute
   dbms_output.put_line(sys.dbms_registry.is_valid('AMD'));
   ```

   If the preceding command returns `0`, then the OLAP CWMLITE tablespace is invalid. Go to step 5.

   If the preceding command returns `1`, then the OLAP CWMLITE tablespace is valid, and no further testing needs to be done.

5. If the OLAP CWMLITE tablespace is invalid, turn on echoing with the following command:

   ```
   SQL> execute cwm2_olap_manager.Set_Echo_on;
   ```

6. Validate the OLAP CMWLITE tablespace with the following command:

   ```
   SQL> execute cwm2_olap_installer.Validate_CWM2_Install;
   ```

After entering the preceding command, the OLAP CWMLITE registry is validated. During this process, screen messages list database objects such as Dimension, Dimension Attribute, and Level, and where these objects are created.

7. When the output stops, enter the following command to verify that the OLAP CWMLITE registry is now valid:

```
SQL> execute
dbms_output.put_line(sys.dbms_registry.is_valid('AMD'));
```

If the preceding command returns `0`, then the OLAP CWMLITE registry is still invalid. Review your installation logs for other errors.

If the preceding command returns 1, then the OLAP CWMLITE tablespace is valid, and no further testing needs to be done.

Oracle9*i* Database Release 2 Product Family

An Oracle White Paper

June 2003

ORACLE

Oracle9*i* Database Release 2 Product Family

INTRODUCTION

Oracle9*i* Database Release 2 is available in three editions, each suitable for different development and deployment scenarios. Oracle also offers several additional optional database products that enhance the capabilities of Oracle9*i* Database for specific application requirements. The following are the three available editions of Oracle9*i* Database Release 2:

- Oracle9*i* Database Standard Edition delivers unprecedented ease-of-use, power, and price/performance for workgroup, department-level, and internet/intranet applications. Oracle9*i* Database Standard Edition includes a fully integrated set of easy-to-use management tools, full distributed, replication, and web features. From single-server environments for small businesses to highly distributed branch environments, Oracle9*i* Database Standard Edition includes all the facilities necessary to build business-critical applications. Oracle9*i* Database Standard Edition can only be licensed on servers that have a maximum capacity of 4 processors.
- Oracle9*i* Database Enterprise Edition provides efficient, reliable, secure data management for high-end applications such as high volume on-line transaction processing (OLTP) environments, query-intensive data warehouses, and demanding Internet applications. Oracle9*i* Database Enterprise Edition provides the tools and functionality to meet the availability and scalability requirements of today's mission-critical applications for the enterprise.
- Oracle9*i* Database Personal Edition supports single user development and deployment that require full compatibility with Oracle9*i* Standard Edition and Oracle9*i* Enterprise Edition. By bringing the award-winning functionality of Oracle9*i* Database to the personal workstation, Oracle offers a database that combines the power of the world's most popular database with the ease of use and simplicity you would expect in a desktop product.

Oracle9*i* Personal Edition, Oracle9*i* Standard Edition and Oracle9*i* Enterprise Edition include a common set of application development features including SQL object-relational capabilities and PL/SQL and Java programmatic interfaces for writing stored procedures and triggers. Applications written for

any edition of Oracle9*i* Database will run with the others, although Oracle9*i* Enterprise Edition provides additional performance, scalability, availability and security functions that are generally transparent to application developers. The APIs supported with Oracle9*i* Enterprise Edition are generally also supported with Oracle9*i* Personal Edition and Oracle9*i* Standard Edition, with exceptions related to the functionality associated with optional additional products only available with Oracle9*i* Personal Edition and Oracle9*i* Enterprise Edition such as Oracle OLAP or Oracle Data Mining.

These Oracle9*i* Database products are all built using the same robust and reliable database engine architecture. Oracle9*i* Database Standard Edition and Oracle9*i* Database Personal Edition are both 100 percent compatible with Oracle9*i* Database Enterprise Edition on many different platforms, so your database applications can scale from the laptop to the desktop to the enterprise without re-engineering.

As your business grows over time, you can easily upgrade from the Oracle9i Database Standard Edition to the Enterprise Edition as your business requires more scalability and functionality. One of the benefits of Oracle SE is that it's so easy to upgrade to EE -- just install the EE software -- you make *no* changes to your database, application, or administrative procedures, and you get all the additional reliability, availability, scalability, and other benefits of EE.

ADVANCED OPTIONS TO MEET DEMANDING REQUIREMENTS

The three Oracle9*i* Database products each have features and functionality to meet the varying requirements of today's applications. Additionally, Oracle offers optional products that contain sophisticated technology to meet your most demanding requirements for development and deployment of mission-critical OLTP, data warehouse, and Internet application environments.

Oracle Real Application Clusters

Oracle Real Application Clusters provides unlimited scalability and high availability for any packaged or custom application by exploiting clustered hardware configurations, with the simplicity and ease of use of a single system image. Oracle Real Application Clusters allows access to a single database from multiple nodes of a clustered system configuration, to insulate application and database users from hardware and software failures, while providing performance that scales with the hardware environment.

Oracle Partitioning

Oracle Partitioning enhances the data management environment for OLTP, data mart, and data warehouse applications by adding significant manageability, availability, and performance capabilities to large underlying database tables and indexes. Oracle Partitioning permits large tables to be broken into individually managed smaller pieces, while retaining a single application-level

view of the data. Range, hash, composite (range combined with hash), and list partitioning methods are supported.

Oracle Advanced Security

Oracle Advanced Security is an Oracle9*i* Enterprise Edition option that provides strong authentication and encryption by implementing industry standard encryption and integrity algorithms as well as supporting several external authentication services. The product provides robust Enterprise User Security where organizations have a choice of implementing end-to-end security by authenticating users using digital certificates or passwords, reducing the total cost of deploying security.

Oracle Label Security

Oracle Label Security provides sophisticated and flexible security based on row labels for fine-grained access control. Oracle Label Security employs labeling concepts used by government, defense and commercial organizations to protect sensitive information and provide data separation and includes a powerful tool to manage policies, labels, and user label authorizations.

Oracle OLAP

Fully integrated in the database, Oracle OLAP provides a complete set of analytical functions. Predictive analysis can be used to forecast market trends, predict product manufacturing requirements, and build enterprise budgeting and financial analysis systems, for example. Using complex, multidimensional queries and calculations, information such as market shares and net present value can be derived. The Java OLAP API provides efficient object-orientation for building applications that require complex analytical queries.

Oracle Data Mining

Oracle Data Mining allows companies to build advanced business intelligence applications that mine corporate databases, discover new insights, and integrate that information into business applications. Oracle Data Mining embeds data mining functionality for making classifications, predictions, and associations. All model-building and scoring functions are accessible through a Java-based API.

Oracle Spatial

Oracle Spatial allows users and application developers to seamlessly integrate their spatial data into enterprise applications. Oracle Spatial facilitates analysis based on the spatial relationships of associated data, like the proximity of store locations to customers within a given distance and sales revenue per territory. Oracle Spatial manages spatial data in an industry-standard database, resulting in application integration that takes place at the data server. This enables

vendor tools and applications to access spatial data directly from Oracle9*i* Database, providing interoperability and minimizing costs.

Oracle Enterprise Manager Packs

In addition to Oracle Enterprise Manager, Oracle provides an advanced integrated package of tools for performance tuning, diagnostics, and change management:

- *Oracle Tuning Pack* - Oracle Tuning Pack provides database administrators with expert performance management for the Oracle environment, including SQL tuning and storage optimization.
- *Oracle Diagnostics Pack* - Oracle Diagnostics Pack enables database administrators to perform advanced monitoring, diagnosis, and planning for the Oracle environment.
- *Oracle Change Management Pack* - Oracle Change Management Pack eliminates errors and loss of data when upgrading databases to support new applications. The pack analyzes the impact and complex dependencies associated with application change and automatically performs database upgrades.
- *Oracle Management Pack for SAP R/3* - Oracle Management Pack for SAP R/3 offers real time monitoring for SAP R/3 systems, capacity planning for historical analysis and future planning purposes, event integration, and a single point of administration of the host, database, and application.

Oracle Programmer

Oracle Programmer is a product that provides a rich set of interfaces for developers who build enterprise applications that access and manipulate Oracle9*i* database.

Oracle Programmer is a family of products consisting of:

- Three embedded SQL-style interfaces: Precompilers, SQL*Module, and SQLJ
- Four call level interfaces: Oracle Call Interface (OCI), Oracle C++ Call Interface (OCCI), ODBC, and JDBC
- Two COM data access interfaces: Oracle Objects for OLE and Oracle Provider for OLE DB
- Microsoft .Net support: Oracle Data Provider for .NET (ODP.NET), OLE DB .NET, and ODBC .NET
- Two utilities to generate host-language bindings from database schemas: Object Type Translator and JPub

FEATURE AND PRODUCT AVAILABILITY

Not all features and options are available with all editions of the Oracle9*i* Database Release 2.

Oracle9*i* Personal Edition is available on Windows2000, Windows NT, Windows XP and Windows Server 2003 (32-bit and 64-bit). It includes at no extra cost all features and options that are available with Oracle9*i* Enterprise Edition, such as Oracle Partitioning and Oracle Advanced Security, with the exception of the Oracle Real Application Clusters option.

See the following table for Oracle9*i* Database Standard Edition and Oracle9*i* Database Enterprise Edition feature and option availability.

Feature/Option	Oracle9*i* Standard Edition	Oracle9*i* Enterprise Edition	Notes
High Availability			
Oracle Data Guard – Redo Apply	N	Y	
Oracle Data Guard – SQL Apply	N	Y	
Basic readable standby database	Y	Y	
Fast-start selectable recovery time	N	Y	
Online index build	N	Y	
Online table reorganization/redefinition	N	Y	
Online index coalesce	N	Y	
Global index maintenance during DDL	Y	Y	
Flashback Query	Y	Y	
Quiesce database	N	Y	
Block-level media recovery	N	Y	
Incremental backup and recovery	N	Y	
Online backup and recovery	Y	Y	
Parallel backup and recovery	N	Y	
Point-in-time tablespace recovery	N	Y	
Trial recovery	N	Y	
Oracle Fail Safe	Y	Y	Windows only

Feature/Option	Oracle9*i* Standard	Oracle9*i* Enterprise	Notes
Transparent application failover	N	Y	
Scalability			
Oracle Real Application Clusters	N	Y	Extra cost option
Cluster File System	N	Y	Requires RAC
Java native compilation	Y	Y	
PL/SQL native compilation	Y	Y	
Security			
Advanced Security Option	N	Y	Extra cost option
Oracle Label Security	N	Y	Extra cost option
Encryption toolkit	Y	Y	
Virtual Private Database	N	Y	
Fine grained auditing	N	Y	
DBA auditing	Y	Y	
Password management	Y	Y	
Proxy authentication	Y	Y	
Development Platform			
Oracle Programmer	Y	Y	Extra cost product
Java support	Y	Y	
SQLJ	Y	Y	Requires Oracle Programmer
JDBC drivers	Y	Y	
XML DB	Y	Y	
Objects and extensibility	Y	Y	
PL/SQL stored procedures and triggers	Y	Y	
PL/SQL Server Pages	Y	Y	
User-defined aggregates	Y	Y	
COM Automation Feature	Y	Y	Windows only

Feature/Option	Oracle9*i* Standard	Oracle9*i* Enterprise	Notes
Microsoft Transaction Server/COM+ integration	Y	Y	Windows only
Oracle OLE DB Provider	Y	Y	Windows only
Oracle Objects for OLE (OO4O)	Y	Y	Windows only
VLM Support	Y	Y	Windows only
OLE DB.NET and ODBC.NET support	Y	Y	Windows only
Native .NET Data Provider – ODP.NET	Y	Y	Windows only
64-bit Itanium support for Windows, Linux, and HP-UX	Y	Y	
Globalization support	Y	Y	
Autonomous transactions	Y	Y	
SQL*Plus	Y	Y	
iSQL*Plus	Y	Y	
Manageability			
Oracle Enterprise Manager	Y	Y	
Oracle Change Management Pack	N	Y	Extra cost option
Oracle Diagnostics Pack	N	Y	Extra cost option
Oracle Tuning Pack	N	Y	Extra cost option
Oracle Management Pack for SAP R/3	N	Y	Extra cost option
Automatic undo management	Y	Y	
Self-tuning memory management	Y	Y	
Server managed backup and recovery	Y	Y	
Recovery Manager	Y	Y	
Legato Storage Manager	Y	Y	
Duplexed backup sets	N	Y	

Feature/Option	Oracle9*i* Standard	Oracle9*i* Enterprise	Notes
Database Resource Manager	N	Y	
Oracle Managed Files	Y	Y	
Locally Managed Tablespaces	Y	Y	
Resumable space allocation	Y	Y	
Unused index identification	Y	Y	
VLDB, Data Warehousing, Business Intelligence			
Oracle Partitioning	N	Y	Extra cost option
Oracle OLAP	N	Y	Extra cost option
Oracle Data Mining	N	Y	Extra cost option
Data Compression	N	Y	
Optimizer statistics management	Y	Y	
Analytic functions	Y	Y	
Bitmapped index and bitmapped join index	N	Y	
Descending index	Y	Y	
Function-based index	Y	Y	
Automated parallel query degree	N	Y	
Parallel statistics gathering	N	Y	
Parallel bitmap star query optimization	N	Y	
Parallel DML	N	Y	No longer requires Partitioning option
Parallel index build	N	Y	
Parallel index scans	N	Y	
Parallel load	Y	Y	
Parallel query	N	Y	
Star query optimization	Y	Y	
Sample scan	Y	Y	

Feature/Option	Oracle9*i* Standard	Oracle9*i* Enterprise	Notes
Summary management	N	Y	
Long operations monitor	Y	Y	
Direct Path Load API	Y	Y	
Export transportable tablespace	N	Y	
Import transportable tablespace	Y	Y	
External tables	Y	Y	
MERGE	Y	Y	
Multi-table insert	Y	Y	
Pipelined table functions	Y	Y	
Synchronous Change Data Capture	N	Y	
Integration			
Oracle Streams	N	Y	
Advanced Queuing	Y	Y	
Oracle Workflow	Y	Y	
Messaging Gateway to IBM MQSeries	N	Y	
Basic Replication	Y	Y	Updatable materialized view site
Advanced Replication	N	Y	Multi-master replication
Distributed queries	Y	Y	
Distributed transactions	Y	Y	
Heterogeneous Services	Y	Y	
Networking			
Connection pooling	Y	Y	
Oracle Connection Manager	N	Y	
Oracle Names	Y	Y	

Feature/Option	Oracle9*i* Standard	Oracle9*i* Enterprise	Notes
Oracle Net Services	Y	Y	
Content Management			
Oracle Spatial	N	Y	Extra cost option
Dynamic Services	Y	Y	
Oracle Database Workspace Manager	Y	Y	
Parallel text index creation	N	Y	
Ultra Search	Y	Y	
*inter*Media	Y	Y	
Oracle Text	Y	Y	
Additional Database Features			
Database event triggers	Y	Y	
DBMS_REPAIR package	Y	Y	
DBMS_METADATA package	Y	Y	
Drop column	Y	Y	
Rename column, constraint	Y	Y	
Index-organized table	Y	Y	
Instead-of triggers	Y	Y	
LOB (large object) support	Y	Y	
Locally-managed tablespaces	Y	Y	
LogMiner	Y	Y	
Multiple block size support	Y	Y	
Plan stability	Y	Y	
Reverse key index	Y	Y	
Temporary table	Y	Y	

Oracle reserves the right to make changes to the contents of this paper at a later date.

ORACLE

Oracle9i Database Product Family
June 2003
Author: Sandra Cheevers
Contributing Authors: Jenny Tsai

Oracle Corporation
World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065
U.S.A.

Worldwide Inquiries:
Phone: +1.650.506.7000
Fax: +1.650.506.7200
www.oracle.com

Oracle Corporation provides the software
that powers the internet.

Technology Foundation

IBM WebSphere Application Server

Product Spec Sheet

The Issue: Meeting Business Objectives in an e-Business World

To create an effective e-business infrastructure, you need more than a Web interface for your J.D. Edwards applications. You need a solid Web infrastructure that is dependable, scalable, and robust enough to handle fluctuating transaction volumes without missing a beat. The infrastructure must also include integrated development tools that allow you to keep your technology solution in line with changing business requirements. Above all, it must be able to meet your current and future enterprise application requirements—right out of the box.

The Solution: WebSphere® Application Server for J.D. Edwards Web Implementations

J.D. Edwards offers the complete end-to-end solution to Web enable your J.D. Edwards applications—J.D. Edwards Technology Foundation. IBM's WebSphere Application Server Advanced Edition 4.0 is bundled with the Technology Foundation to provide the ideal platform for your J.D. Edwards Web applications. Together, the WebSphere Application Server and J.D. Edwards' Web-enabled applications create a comprehensive, enterprise-class solution that offers flexibility, scalability, security, ease of use, and a lower total cost of ownership, while supplying you with industry-leading functionality and performance.

Tightly integrated with sophisticated development tools, the WebSphere Application Server provides advanced integration capabilities based on open, industry-standard technologies. It allows you to leverage existing IT assets by connecting to a variety of databases and platforms.

With the WebSphere Application Server, you are able to:

- Make changes in application logic without reworking code, even while the application is running.
- Efficiently share dynamic customer information from one end of a distributed application to the other.
- Deploy applications based on the Java 2 Platform, Enterprise Edition (J2EE) standard that intelligently adjust presentation and business logic for different client locales and time zones.
- Increase availability by scaling through horizontal or vertical cloning.
- Integrate enterprise information systems as reusable business services.
- Connect with existing Microsoft®, Common Object Request Broker Architecture (CORBA), and C++ applications.
- Handle business events through advanced messaging technology.

Feature/Function Highlights

- J2EE compliance
- Java technology foundation
- Firewall support
- Browser-based administration tools
- Internationalization services
- Extended messaging support
- Built-in process engine
- Business rules support
- Shared work areas
- Bidirectional CORBA connectivity
- C++ CORBA software developer's kit
- ActiveX bridge
- High-speed transaction processing support

Platform Operating Systems Support

- AIX 4.3.3 and 5.1
- HP-UX 11.0 and 11i (or 11.11)
- Solaris 7 and 8
- Windows 2000 SP3 and Advanced Server SP3
- AS/400 V5R1 and V5R2

JDEDWARDS
you > us

www.jdedwards.com

Lower Your Total Cost of Ownership

As part of the J.D. Edwards Technology Foundation, the WebSphere Application Server offers a cost-effective and efficient way for you to deploy J.D. Edwards applications.

By purchasing the WebSphere Application Server as part of the J.D. Edwards Technology Foundation, you save time and money through application pre-integration. And with J.D. Edwards as your complete solution vendor, you benefit from further cost savings by having a single source for service and support, rather than having multiple vendors.

The WebSphere Application Server also saves costs by simplifying administration and systems management. It provides a central and open management interface to help you administer multiple applications and components from the same environment. Built-in set-up options and administrative features aid in application deployment and administration, while automated management functions enhance productivity and reduce administrative costs.

Enhance Flexibility

With multiple configuration options, the WebSphere Application Server supports a wide range of scenarios, from simple administration of a single server to a clustered, high-availability, high-volume environment. The specialized configuration options give you the flexibility to respond to an ever-changing market—without the costs of migrating to a different technology base.

Support Enterprise Needs

With J.D. Edwards and the WebSphere Application Server, you are able to extend your enterprise applications to the Web, efficiently and cost effectively. With scalability built in—through such capabilities as cloning, for example—the WebSphere Application Server can be used in a variety of environments. To help in large installations, J.D. Edwards' customers can take advantage of the IBM EdgeServer*. By supporting dynamic load balancing between physical Web servers, it is ideal for larger enterprise environments.

With the WebSphere Application Server, you benefit from a flexible infrastructure that offers unmatched functionality and stability and is easy to deploy and support. Delivered by two industry leaders, the WebSphere Application Server, as part of the Technology Foundation, is built to support your business needs.

J.D. Edwards: A Strategic Partner for Your Long-term Needs

A solution is only as good as the company that stands behind it. That is why J.D. Edwards is committed to innovation, superior value, and customer satisfaction. Our singular goal is to help make you stronger, enabling you to solve your most important business challenges. We do this by dedicating ourselves to continually enhancing the value of our solutions, not only with software research and development, but also with superior consulting, education, and training support. As your long-term business partner, J.D. Edwards will work with you to help ensure that our solutions grow and change with your business—making your technology investment an asset that increases in value over time.

*EdgeServer is not included in the J.D. Edwards Technology Foundation product offering, but is available through IBM or an IBM channel reseller.

Database Support

- UNIX
- UDB 7.2 FP 5 or 7
- Oracle 8.1.7.3 or 4 and 9.0.1.4
- Windows
- UDB 7.2 FP 5 or 7
- Oracle 8.1.7.3 or 4 and 9.0.1.4
- SQL 2000 SP3
- AS/400 DB2 for iSeries

Solution Integration

- ERP
- CRM
- Supply Chain Management
- Supplier Relationship Management
- Business Intelligence
- Collaborative Portal

J.D. Edwards
World Headquarters
One Technology Way
Denver, Colorado 80237, USA
800 727 5333 / 303 334 4000
www.jdedwards.com

J.D. Edwards (UK) Ltd.
Europe, the Middle East, and Africa
Colorado House
300 Thames Valley Park Drive
Reading
Berkshire RG6 1RD, UK
044 1189 091 700
www.jdedwards.co.uk

J.D. Edwards
Latin America and the Caribbean
806 Douglas Entrance, Suite 570
Coral Gables, Florida 33134, USA
305 442 7800
www.jdedwards.com.mx

J.D. Edwards (Asia Pacific) Pte Ltd.
No. 1 International Business Park
The Synergy, #06-01/04
Singapore 609917
65 227 3391
www.jdedwards.com.tw

March 2003

WASpse.0303

24.556
J.

gerenciamento SNMP
2 Fontes de Alimentação operando de forma redundante

SERVIDOR INTEL TIPO 2
CCD/BSB:29, CCD/SP:6
HP Proliant DL 580 G2 montado em rack
4 processadores Intel Xeon MP de 2.0 Ghz
Barramento de sistema de 400 Mhz
Memória cache de 2Mb por processador
Memória RAM de 4Gb ECC SDRAM
Controladora integrada Ultra 3 SCSI com suporte a RAID 0, 1, 0+1, 5
2 discos rígidos SCSI Ultra 3 de 10K rpm de 72,8 Gb – Hot Swap
Controladora de vídeo SVGA integrada com 8Mb
Uma unidade de CD-ROM IDE 24 X
2 controladoras Fiber Channel operando a 2 GB com 2 canais
2 interfaces de rede local em barramento PCI padrão Ethernet 10/100/1000 Base-T com gerenciamento SNMP
2 Fontes de Alimentação operando de forma redundante

SERVIDOR INTEL TIPO 3
CCD/BSB:27, CCD/SP:24
HP Proliant DL 380 G3 montado em rack
2 processadores Intel Xeon de 3.06 Ghz
Barramento de sistema de 533 Mhz
Memória cache de 512 Kb por processador
Memória RAM de 2Gb ECC SDRAM
Controladora integrada Ultra 3 SCSI com suporte a RAID 0, 1, 0+1, 5
2 discos rígidos SCSI Ultra 3 de 10K rpm de 72,8 Gb – Hot Swap
Controladora de vídeo SVGA integrada com 8Mb
Uma unidade de CD-ROM IDE 24 X
2 interfaces de rede local em barramento PCI padrão Ethernet 10/100/1000 Base-T com gerenciamento SNMP
2 Fontes de Alimentação operando de forma redundante
HP Proliant DL 380 G3 montado em rack

SERVIDOR RISC TIPO 01
CCD/BSB:8, CCD/SP:3
11 x Servidores RISC Tipo 01, modelo SuperDome com a seguinte configuração por Servidor:
24 x CPU PA-RISC PA8700 de 875 MHz e 2,25 MB de memória cache L1
64 Gbytes de memória RAM
04 x Placa PCI Core I/O com uma interface 100 BT Ethernet
16 x Placa PCI com uma interface 10/100/1000BaseT Ethernet LAN
16 x Placa PCI com uma interface Fiber Channel de 2GB/s
08 x Placa PCI com duas interfaces U160 LVD/SE SCSI
04 x Placa PCI com 2 portas Ultra-2 SCSI e 2 portas 100BaseT
24 x licença de 1 CPU para HP-UX 11i
24 x licença de 1 CPU para HP-UX Virtual Partitions (vPar)
24 x licenças de 1 CPU para Online JFS
24 x licenças de 1 CPU para MirrorDisk/UX
06 fontes independentes e redundantes, configuradas para atender a capacidade máxima de expansão solicitada , com alimentação redundante através de 2 (dois) circuitos.
16 x Gabinete de disco HP SureStore DS2100 montados em rack

14.555
A.

DESCRIÇÃO TÉCNICA POR TIPO DE EQUIPAMENTO

SWTCH TIPO 4 (KVM)	
Switch KVM - Solução DF	
Fabricante	BlackBox
Modelo	AFFINITY
Total de Portas	160
Rack BlackBox Padrão 19" 40 U de altura	01
Monitor Compaq S7500 17"	08
Teclado PS/2	08
Mouse PS/2	08
*Todos os cabos necessários para a instalação, estão inclusos na proposta.	
Switch KVM - Solução SP	
Fabricante	BlackBox
Modelo	AFFINITY
Total de Portas	96
Rack BlackBox Padrão 19" 40 U de altura	01
Monitor Compaq S7500 17"	04
Teclado PS/2	04
Mouse PS/2	04
*Todos os cabos necessários para a instalação, estão inclusos na proposta.	

SWITCH TIPO 3
CCD/BSB
02 EMC Racks EC-1230B
04 (quatro) Directors Fibre Channel EMC Connectrix ED-12000B com 64 portas FibreChannel 2Gbit/s cada
Total de 256 portas FibreChannel de 2Gbit/s
308 (trezentos e oito) cabos FibreChannel de 50 metros
Software Fabric OS, Fabric Manager e Fabric Watch
CCD-SP
01 EMC Rack EC-1230B
02 (quatro) Directors Fibre Channel EMC Connectrix ED-12000B com 64 portas FibreChannel 2Gbit/s cada
Total de 128 portas FibreChannel de 2Gbit/s
154 (cento e cinquent e quatro) cabos FibreChannel de 50 metros
Software Fabric OS, Fabric Manager e Fabric Watch

SERVIDOR INTEL TIPO 1
CCD/BSB:14, CCD/SP:7
HP Proliant DL 760 G2 montado em rack
8 processadores Intel Xeon MP de 2.0 Ghz
Barramento de sistema de 400 Mhz
Memória cache de 2Mb por processador
Memória RAM de 8Gb ECC SDRAM
Controladora integrada Ultra 3 SCSI com suporte a RAID 0, 1, 0+1, 5
2 discos rígidos SCSI Ultra 3 de 10K rpm de 72,8 Gb – Hot Swap
Controladora de vídeo SVGA integrada com 8Mb
Uma unidade de CD-ROM IDE 24 X
2 controladoras Fiber Channel operando a 2 GB com 2 canais
3 interfaces de rede local em barramento PCI padrão Ethernet 10/100/1000 Base-T com

16 x Disco de 36GB 10K, para DS2100
02 x Gabinete para dispositivos HP SureStore TA5300 para rack
02 x HP SureStore DVD-ROM para TA5300
02 x HP SureStore DAT 24 DDS-3 para TA5300
40 x Fitas novas padrão DDS-3
08 x Fitas novas para limpeza.
Adicionais:
240 x licenças de 1 CPU para MC/ServiceGuard extensão para Oracle 9i Real Application Cluster - RAC ou Oracle 8i Parallel Server - OPS, permitindo a criação de até 10 partições ,em Servidores RISC Tipo 1, com Oracle 9i Real Application Cluster - RAC ou Oracle 8i Parallel Server - OPS.
144 x licenças de 1 CPU para Compilador C padrão ANSI C, totalizando a quantidade 6 servidores RISC Tipo 1 com compilador C padrão C/ANSI para número de usuários ilimitados.
09 x Rack HP de 41 U padrão 19"
04 x Console rp2470 ,2 (duas) para cada localidade, para gerenciamento de todos os equipamentos em cada localidade e criação/gerenciamento das partições
Observações:
Para criação de uma partição virtual é necessário uma CPU, um disco de boot , 2 GB de memória e uma interface SI, desta forma, atendemos a capacidade de criação de no mínimo 8 partições lógicas, expansível a no mínimo (dezesseis) partições lógicas.

JD Edwards' OneWorld Xe Implementation and Certification With Hewlett-Packard's MC/ServiceGuard High Availability Software

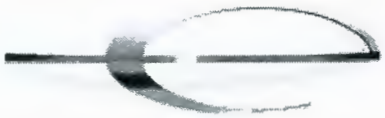
JD Edwards Home Page

The HP Partner Technology Center (PTAC) has successfully integrated OneWorld Xe with MC/ServiceGuard. The implementation and certification of OneWorld Xe followed the PTAC's High Availability Implementation and Certification Process.

Information regarding this process, and how other ISVs may take advantage of this service, is available in these PTAC documents:

Appendix 33: HP's Partner Technology Access Center High Availability Implementation and Certification Services Datasheet

Appendix 34: HP's Partner Technology Access Center High Availability Implementation and Certification Services Process and Methodology



JDEDWARDS®

Executive Overview

JD Edwards and OneWorld Xe

With approximately 5,700 customers and 5,000 employees — as well as $944 million in revenue in fiscal year 1999 — J.D. Edwards (NASDAQ: JDEC) is the leading supplier of e-business solutions that deliver speed and agility for customers throughout the world. For more than 20 years, J.D. Edwards has provided innovative, flexible solutions essential to running complex and fast-moving multinational organizations — acting as a true business partner to help companies of all sizes leverage existing investments, take advantage of new technologies, and maintain competitive advantage.

What most distinguishes J.D. Edwards is its customer-centric Idea to Action™ value proposition, an industry-redefining approach to collaborative business software solutions. Idea to Action helps you use information technology efficiently throughout the virtual enterprise, easily tailoring applications to meet changing business needs. It gives you the freedom to put your ideas into action quickly in a B2B world.

OneWorld® Xe, the company's new "extended enterprise" product, boasts some 300 Internet-ready applications that enable companies to choose the most appropriate collaborative solutions to meet their business needs.

OneWorld Xe, with capabilities enhanced via J.D. Edwards' eXtended Process Integration (XPI) engine, will allow customers to use open, flexible and interoperable technologies that foster communication and commerce among suppliers and customers across their extended supply chain.

With OneWorld Xe's key defined areas of functionality — ranging from customer relationship management to integrated supply chain and fulfillment management — J.D. Edwards customers can optimize a factory, a distribution channel or an entire supply chain network.

"We have already seen tremendous customer demand for OneWorld Xe," said Glenn Tubb, senior vice president of development of J.D. Edwards. "Giving our customers open collaboration is empowering them to automate and streamline business processes across the supply chain to increase shareholder value and optimize working capital."

Currently, J.D. Edwards has over 1,000 customers that are live on various releases of OneWorld as well as dozens of OneWorld Xe customers who have been using the product in beta form. Beta customers on OneWorld Xe include Praxair, a $4.7 billion global pioneer in the industrial gases industry; Ontario Store Fixtures, the leading North American manufacturer of complete retail store interiors; Grupo LaLa, a Mexican holding company in the food industry; Fisher & Paykel Industries Ltd., a New Zealand-based manufacturer of home appliances and healthcare items; and Cascade Designs, a manufacturer of outdoor, travel, and wheel chair cushion products.

Richest Functionality

J.D. Edwards' OneWorld Xe combines the best of back office software, enterprise applications integration (EAI) and inter-enterprise process workflow into one solution, with new features that achieve the following benefits:

- Lasting Value. OneWorld's event-driven, component-based architecture is enhanced to increase reach and agility. OneWorld Xe automatically generates intuitive Windows, HTML and Java user interfaces from one set of business specifications, allowing users to choose their interface of choice. Its configurable, Web-based portal serves as the single point of entry into OneWorld and can be tailored to meet the access and collaboration needs of partners, suppliers and customers. With intuitive change management capabilities, OneWorld Xe allows users to make changes to existing processes, activate additional capabilities or manage upgrades.
- Collaboration based on standards-based interoperability. OneWorld Xe supports XML-based business-to-business interoperability technology from Netfish, and enterprise application technology from Active Software (a.k.a. WebMethods). J.D. Edwards is embedding these technologies into its eXtended

Process Integration engine, OneWorld XPI, which will serve as the integration platform or "broker" that addresses both internal enterprise application portfolios and external interoperability with customers' and trading partners' business systems.

- Freedom to Choose pre-integrated e-business applications. With OneWorld Xe, J.D. Edwards tightens integration with strategic partner solutions and delivers notable new and enhanced functionality, including:
- Enhanced advanced planning, providing best-in-class collaboration, real-time order promising, and new functionality for discrete industries.
- An intelligent, role- and relationship-based messaging which will support real-time collaboration among multiple trading community partners.
- Web-enabled demand planning module for collaboration on forecasts and improved geographical mapping capabilities to more accurately represent facility locations.
- New storefront options with Microsoft Commerce Server and IBM WebSphere Commerce Suite, which are pre-integrated with OneWorld Xe.
- Knowledge management solution (slated for availability in early 2001) for gathering data from document repositories, Intranets, data warehouses, supply chains and the Internet and delivering it to employees, partners and customers for integrated decision support. Using data warehouse development tools, any database can be used as a business intelligence source. New and updated information is automatically pushed to users' desktop, phone, fax, wireless device or OneWorld portal.
- Application integrations to deliver extended solutions, including Siebel eConsumer Goods in J.D. Edwards Solutions for Consumer Industries; Extensity time, travel and expense management; and Ariba Buyer.
- Self-service options to increase productivity and improve response with secure, self-service portals that automate most routine query-and-update tasks. Managers can initiate personnel actions; suppliers can respond to quotes, initiate date change requests, inquire on orders, receipts, inventory levels and payment information; and carriers can inquire on assigned loads and shipments.

High Availability with HP MC/ServiceGuard

HP Multi-Computer/ServiceGuard (MC/ServiceGuard) is a specialized facility for protecting mission-critical applications from a wide variety of hardware and software failures. With MC/ServiceGuard, multiple— up to 16—nodes (systems) are organized into an enterprise cluster that delivers highly available application services to LAN-attached clients.

HP MC/ServiceGuard monitors the health of each node and quickly responds to failures in a way that minimizes or eliminates application downtime. MC/ServiceGuard is able to automatically detect and respond to failures in the following components:

- System processors
- System memory
- LAN media and adapters
- System processes
- Application processes

Application Packages
With HP MC/ServiceGuard, application services and all the resources needed to support the application are bundled into special entities called application packages. These application packages are the basic units that are managed and moved within an enterprise cluster. Packages simplify the creation and management of highly available services and provide outstanding levels of flexibility for workload balancing.

Fast Detection of Failure, Fast Restoration of Applications
Within an enterprise cluster, HP MC/ServiceGuard monitors hardware and software components, detects failures, and responds by promptly allocating new resources to support mission-critical applications. The process of detecting the failure and restoring the application service is completely automated—no operator intervention is needed.

Recovery times provided by HP MC/ServiceGuard for LAN adapter failures are extremely fast, typically within a few seconds. Recovery times for failures requiring the switch of an application to an alternate node will vary, depending on the software services being used by the application. For example, a database application that is using a logging facility would need to perform transaction rollbacks as part of the recovery process. The time needed to perform this transaction rollback would be part of the total time to recover the application. MC/ServiceGuard will detect the node failure, reconfigure the cluster, and begin executing the startup script for the application package on an alternate node in less than 30 seconds.

High Availability for Mission-Critical Applications

99.95% Uptime Commitment—The Mission-Critical Server Suites (MCSS) is HP's platform solution, offering an unprecedented 99.95% uptime commitment. Pre-configured and tested, MCSS is based on MC/ServiceGuard-enabled HP 9000 Enterprise Servers, packaged with the consulting and support services necessary to ensure success in your mission-critical environment.

MCSS solutions are available on HP 9000 R-, L-, N-, K-, and V-Class servers; and high availability storage is offered on either disk arrays with AutoRAID, or the HP SureStore E XP256 or XP512, providing the ultimate in data availability, reliability, and high performance.

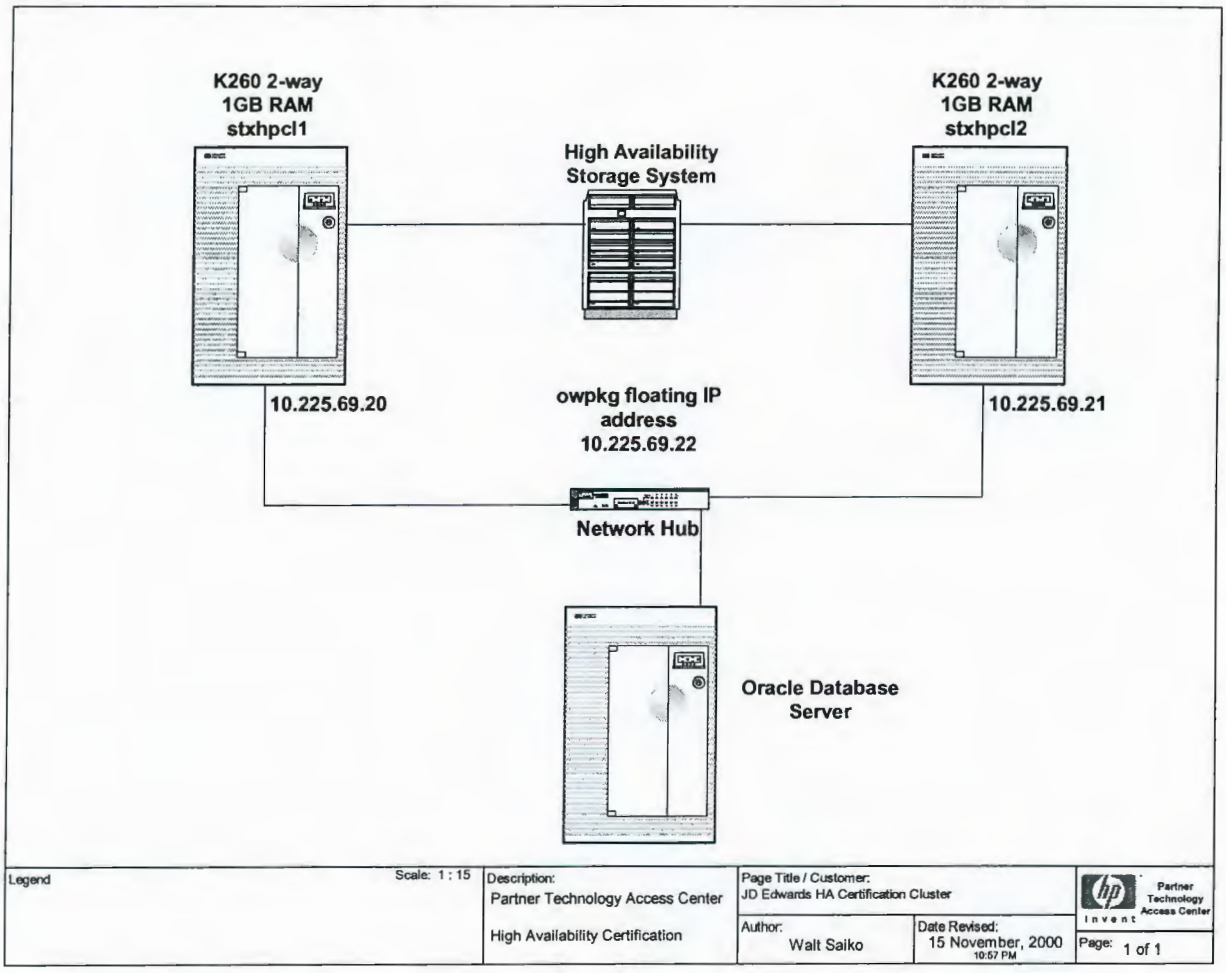
Other Benefits of MC/ServiceGuard:
-Availability during Hardware and Software Maintenance
-Online Reconfiguration Reduces Planned Downtime
-Workload Balancing
-Protecting Data Integrity

For more information, contact any of our worldwide sales offices or HP Channel Partners (in the U.S. call 1-800-637-7740).

OneWorld Xe in a Highly-Available Environment

Integrating OneWorld Xe with MC/ServiceGuard provides redundancy and high availability for OneWorld Xe. This integration provides:

- minimal downtime in the event of a system failure
- automatic response to the user interface that owns running OneWorld batch jobs
- minimal delay before running OneWorld batch jobs are able to be restarted
- no reconfiguration of clients in a client/server environment; the ServiceGuard movement of the OneWorld server to another physical node is transparent to the client nodes.



In the first configuration tested, one primary node was used (stxhpcl1), with a second node initially not performing any OneWorld-related activity (stxhpcl2) (standby node). Both the active and standby nodes were connected to a High Availability Storage System (HASS) disk storage mechanism via FWD SCSI connection. The HASS contained the MC/ServiceGuard cluster lock disk, shared OneWorld Xe files and instance information needed by both the primary OneWorld node and the standby OneWorld node (upon a failover).

An additional node was part of this configuration. This node was configured as an Oracle Database Server. The Oracle Database has been previously certified as compatible with MC/ServiceGuard; thus, for this certification effort, it was decided that only OneWorld Xe would be configured in a failover architecture.

A remote node was connected via TCP/IP LAN to the same subnet as stxhpcl1 and stxhpcl2. This remote node, running Windows NT, was used to run the OneWorld Xe client software. This node was the source of client/server requests to the OneWorld Xe server, and was also used to submit batch jobs to the OneWorld Xe server.

Two different configurations were tested and certified:

Configuration #1 – A Single Instance of OneWorld Xe, running on one machine, with a dedicated standby machine.

- One package was created. This package mounted the shared volume group and file systems. The package then performed a set user (su) command, invoked the OneWorld environment, and ran the script to start OneWorld.

- A monitor script was written to monitor the jdenet_n and jdequeue processes. The script is run by MC/ServiceGuard during package start. The monitor script will stay in a loop, checking for the existence of these processes. If either or both of these processes do not exist, a failover scenario will be initiated.

- A HA Monitor was configured as part of the package, to monitor the available filesystem size of the OneWorld filesystems. This monitor was maintained by MC/ServiceGuard. If the available filesystem size dropped below 5% for any of the shared filesystems, MC/ServiceGuard would report this error, and initiate a failover scenario. This monitor was also configured as a package dependency, i.e. the package depended upon this filesystem resource to perform its work. If the filesystem resource was not available, the package would not start.

Configuration #2 – Two Instances of OneWorld Xe, each running on a separate machine, with each machine being able to failover to the other.

- Two packages were created, owpkg1 and owpkg2. Package owpkg1 is primary on node stxhpcl1 while package owpkg2 is primary on node stxhpcl2. Each package mounts a shared volume group and separate file system. Each package then performed a set user (su) command, invoked the OneWorld environment, and ran the script to start OneWorld.

- Once both packages had been started by MC/ServiceGuard, two separate and operational instances of OneWorld Xe were running. Each instance had its own IP address, own volume group and own file system. In actual operation, one OneWorld instance could have been used for interactive operation, while the other instance could have been used for batch operations.

- Each instance of OneWorld Xe accessed a common database owned by the Oracle Database Server, which was described earlier within this document.

- A monitor script was written to monitor the jdenet_n and jdequeue processes. The script is run by MC/ServiceGuard during package start. The monitor script will stay in a loop, checking for the existence of these processes. If either or both of these processes do not exist, a failover scenario for that package will be initiated.

- A HA Monitor was configured as part of the package, to monitor the available filesystem size of the OneWorld filesystems. This monitor was maintained by MC/ServiceGuard. If the available filesystem size on either machine dropped below 5% for any of the shared filesystems, MC/ServiceGuard would report this error, and initiate a failover scenario for that package. This monitor was also configured as a package dependency, i.e. the package depended upon this filesystem resource to perform its work. If the filesystem resource was not available, the package would not start.

The OneWorld Xe application is validated and certified by Hewlett-Packard as compatible with Hewlett-Packard's MC/ServiceGuard high availability software. OneWorld Xe can be monitored by MC/ServiceGuard, with the level of monitoring highly configurable and subject to the implementation plans of the customer.

This document details a set of tests showing that OneWorld Xe is compatible with MC/ServiceGuard. The tests show that if a node running a OneWorld Xe batch job fails, the job can be restarted on an alternate node in less than 30 seconds. Also, any client-server connections to failed OneWorld Xe processes can be reconnected to the OneWorld server running on an alternate node.

MC/ServiceGuard packages are dependent on having automated application startup and shutdown scripts. HP engineers have developed package configuration and control scripts that are suitable for use (after system-specific modification) in a OneWorld Xe production environment.

OneWorld Xe Implementation and Certification in an MC/ServiceGuard Cluster

The process followed for the certification of OneWorld Xe in an MC/ServiceGuard environment is detailed in:

Appendix 34: HP's Partner Technology Access Center High Availability Implementation and Certification Services Process and Methodology

Implementation and Certification Onsite Process Participants:

Hewlett-Packard: Walt Saiko (Partner Technology Access Center)
JD Edwards: Roger Miller (Server Technology)

MC/ServiceGuard Configuration

Configuration 1 – Single Instance of OneWorld Xe

Configuring the Cluster

Create the ASCII cluster template file

```
cmquerycl –v –C /etc/cmcluster/cluster1.ascii –n stxhpcl1 –n stxhpcl2
```

Modify the template (cluster1.ascii) to reflect the environment and to verify the cluster configuration.

```
cmcheckconf –v –C /etc/cmcluster/cmclconfig.ascii
```

Create the cluster by applying the configuration file. This will create the binary file "cmclconfig" and automatically distribute it among the nodes defined in the cluster.

```
cmapplyconf –v –C /etc/cmcluster/cmclconfig.ascii
```

Start the cluster and check the cluster status. Test the cluster halt also.

```
cmruncl –v –n stxhpcl1 –n stxhpcl2
cmviewcl –v
cmhaltcl –f –v
cmruncl –n stxhpcl1 –n stxhpcl2
```

Configuring a ServiceGuard Package on the Primary Node.

Create the package configuration files and tailor to the test environment. Do not include the second node at this stage.

```
cd /etc/cmcluster
mkdir owpkg
cmmakepkg –p owpkg.ascii          # Edit owpkg.ascii
```

Create package control scripts and tailor to the test environment. Do not include application startup/shutdown, service monitoring, or relocatable IP address at this stage.

```
cd owpkg
cmmakepkg –s control.sh
```

Shut down cluster, verify and distribute the binary configuration files

```
cmhaltcl –f –v
cmapplyconf –v –C /etc/cmcluster/cmclconfig.ascii –P owpkg.ascii
```

Test cluster and package startup. Unmount all logical volumes on shared volume group and deactivate the volume group

```
cmruncl                           # Start cluster and package
cmviewcl –v                       # Check that package has started
```

Add knowledge of the Secondary Node to the packages

```
edit owpkg.ascii
```

Shut down cluster, verify and distribute the binary configuration files

```
cmhaltcl –f –v
cmapplyconf –v –C /etc/cmcluster/cmclconfig.ascii –P owpkg.ascii
```

Test cluster and package startup.. Unmount all logical volumes on shared volume group and deactivate the volume group

```
cmruncl                           # Start cluster and package
cmviewcl –v                       # Check that package has started
```

JD Edwards' OneWorld Xe Implementation and Certification With Hewlett-Packard's MC/ServiceGuard High Availability Software

JD Edwards Home Page

The HP Partner Technology Center (PTAC) has successfully integrated OneWorld Xe with MC/ServiceGuard. The implementation and certification of OneWorld Xe followed the PTAC's High Availability Implementation and Certification Process.

Information regarding this process, and how other ISVs may take advantage of this service, is available in these PTAC documents:

Appendix 33: HP's Partner Technology Access Center High Availability Implementation and Certification Services Datasheet

Appendix 34: HP's Partner Technology Access Center High Availability Implementation and Certification Services Process and Methodology

Executive Overview

JD Edwards and OneWorld Xe

With approximately 5,700 customers and 5,000 employees — as well as $944 million in revenue in fiscal year 1999 — J.D. Edwards (NASDAQ: JDEC) is the leading supplier of e-business solutions that deliver speed and agility for customers throughout the world. For more than 20 years, J.D. Edwards has provided innovative, flexible solutions essential to running complex and fast-moving multinational organizations — acting as a true business partner to help companies of all sizes leverage existing investments, take advantage of new technologies, and maintain competitive advantage.

What most distinguishes J.D. Edwards is its customer-centric Idea to Action™ value proposition, an industry-redefining approach to collaborative business software solutions. Idea to Action helps you use information technology efficiently throughout the virtual enterprise, easily tailoring applications to meet changing business needs. It gives you the freedom to put your ideas into action quickly in a B2B world.

OneWorld® Xe, the company's new "extended enterprise" product, boasts some 300 Internet-ready applications that enable companies to choose the most appropriate collaborative solutions to meet their business needs.

OneWorld Xe, with capabilities enhanced via J.D. Edwards' eXtended Process Integration (XPI) engine, will allow customers to use open, flexible and interoperable technologies that foster communication and commerce among suppliers and customers across their extended supply chain.

With OneWorld Xe's key defined areas of functionality — ranging from customer relationship management to integrated supply chain and fulfillment management — J.D. Edwards customers can optimize a factory, a distribution channel or an entire supply chain network.

"We have already seen tremendous customer demand for OneWorld Xe," said Glenn Tubb, senior vice president of development of J.D. Edwards. "Giving our customers open collaboration is empowering them to automate and streamline business processes across the supply chain to increase shareholder value and optimize working capital."

Currently, J.D. Edwards has over 1,000 customers that are live on various releases of OneWorld as well as dozens of OneWorld Xe customers who have been using the product in beta form. Beta customers on OneWorld Xe include Praxair, a $4.7 billion global pioneer in the industrial gases industry; Ontario Store Fixtures, the leading North American manufacturer of complete retail store interiors; Grupo LaLa, a Mexican holding company in the food industry; Fisher & Paykel Industries Ltd., a New Zealand-based manufacturer of home appliances and healthcare items; and Cascade Designs, a manufacturer of outdoor, travel, and wheel chair cushion products.

Richest Functionality

J.D. Edwards' OneWorld Xe combines the best of back office software, enterprise applications integration (EAI) and inter-enterprise process workflow into one solution, with new features that achieve the following benefits:

- Lasting Value. OneWorld's event-driven, component-based architecture is enhanced to increase reach and agility. OneWorld Xe automatically generates intuitive Windows, HTML and Java user interfaces from one set of business specifications, allowing users to choose their interface of choice. Its configurable, Web-based portal serves as the single point of entry into OneWorld and can be tailored to meet the access and collaboration needs of partners, suppliers and customers. With intuitive change management capabilities, OneWorld Xe allows users to make changes to existing processes, activate additional capabilities or manage upgrades.
- Collaboration based on standards-based interoperability. OneWorld Xe supports XML-based business-to-business interoperability technology from Netfish, and enterprise application technology from Active Software (a.k.a. WebMethods). J.D. Edwards is embedding these technologies into its eXtended

Process Integration engine, OneWorld XPI, which will serve as the integration platform or "broker" that addresses both internal enterprise application portfolios and external interoperability with customers' and trading partners' business systems.

- Freedom to Choose pre-integrated e-business applications. With OneWorld Xe, J.D. Edwards tightens integration with strategic partner solutions and delivers notable new and enhanced functionality, including:
- Enhanced advanced planning, providing best-in-class collaboration, real-time order promising, and new functionality for discrete industries.
- An intelligent, role- and relationship-based messaging which will support real-time collaboration among multiple trading community partners.
- Web-enabled demand planning module for collaboration on forecasts and improved geographical mapping capabilities to more accurately represent facility locations.
- New storefront options with Microsoft Commerce Server and IBM WebSphere Commerce Suite, which are pre-integrated with OneWorld Xe.
- Knowledge management solution (slated for availability in early 2001) for gathering data from document repositories, Intranets, data warehouses, supply chains and the Internet and delivering it to employees, partners and customers for integrated decision support. Using data warehouse development tools, any database can be used as a business intelligence source. New and updated information is automatically pushed to users' desktop, phone, fax, wireless device or OneWorld portal.
- Application integrations to deliver extended solutions, including Siebel eConsumer Goods in J.D. Edwards Solutions for Consumer Industries; Extensity time, travel and expense management; and Ariba Buyer.
- Self-service options to increase productivity and improve response with secure, self-service portals that automate most routine query-and-update tasks. Managers can initiate personnel actions; suppliers can respond to quotes, initiate date change requests, inquire on orders, receipts, inventory levels and payment information; and carriers can inquire on assigned loads and shipments.

24.541
A.

High Availability with HP MC/ServiceGuard

HP Multi-Computer/ServiceGuard (MC/ServiceGuard) is a specialized facility for protecting mission-critical applications from a wide variety of hardware and software failures. With MC/ServiceGuard, multiple— up to 16—nodes (systems) are organized into an enterprise cluster that delivers highly available application services to LAN-attached clients.

HP MC/ServiceGuard monitors the health of each node and quickly responds to failures in a way that minimizes or eliminates application downtime. MC/ServiceGuard is able to automatically detect and respond to failures in the following components:

- System processors
- System memory
- LAN media and adapters
- System processes
- Application processes

Application Packages
With HP MC/ServiceGuard, application services and all the resources needed to support the application are bundled into special entities called application packages. These application packages are the basic units that are managed and moved within an enterprise cluster. Packages simplify the creation and management of highly available services and provide outstanding levels of flexibility for workload balancing.

Fast Detection of Failure, Fast Restoration of Applications
Within an enterprise cluster, HP MC/ServiceGuard monitors hardware and software components, detects failures, and responds by promptly allocating new resources to support mission-critical applications. The process of detecting the failure and restoring the application service is completely automated—no operator intervention is needed.

Recovery times provided by HP MC/ServiceGuard for LAN adapter failures are extremely fast, typically within a few seconds. Recovery times for failures requiring the switch of an application to an alternate node will vary, depending on the software services being used by the application. For example, a database application that is using a logging facility would need to perform transaction rollbacks as part of the recovery process. The time needed to perform this transaction rollback would be part of the total time to recover the application. MC/ServiceGuard will detect the node failure, reconfigure the cluster, and begin executing the startup script for the application package on an alternate node in less than 30 seconds.

High Availability for Mission-Critical Applications

99.95% Uptime Commitment—The Mission-Critical Server Suites (MCSS) is HP's platform solution, offering an unprecedented 99.95% uptime commitment. Pre-configured and tested, MCSS is based on MC/ServiceGuard-enabled HP 9000 Enterprise Servers, packaged with the consulting and support services necessary to ensure success in your mission-critical environment.

MCSS solutions are available on HP 9000 R-, L-, N-, K-, and V-Class servers; and high availability storage is offered on either disk arrays with AutoRAID, or the HP SureStore E XP256 or XP512, providing the ultimate in data availability, reliability, and high performance.

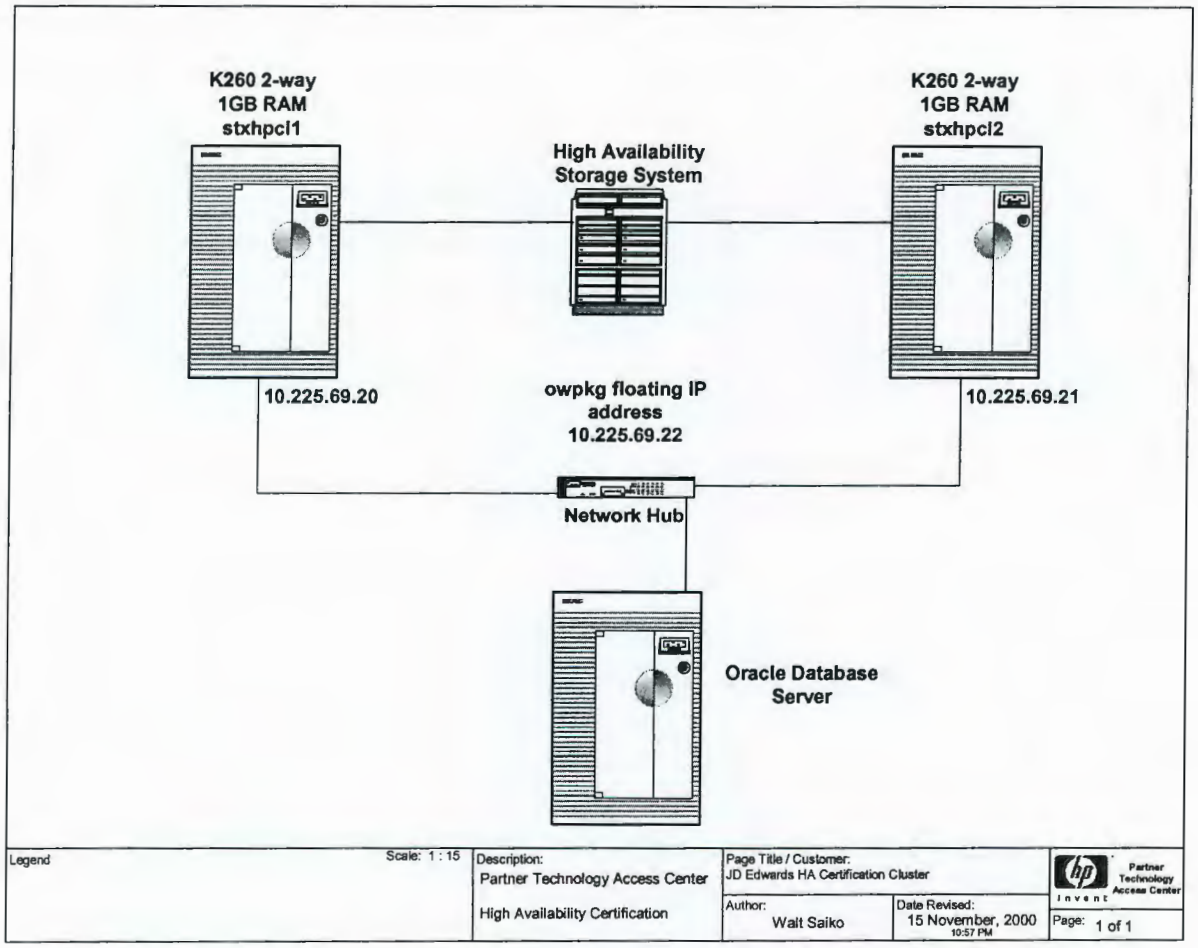
Other Benefits of MC/ServiceGuard:
-Availability during Hardware and Software Maintenance
-Online Reconfiguration Reduces Planned Downtime
-Workload Balancing
-Protecting Data Integrity

For more information, contact any of our worldwide sales offices or HP Channel Partners (in the U.S. call 1-800-637-7740).

OneWorld Xe in a Highly-Available Environment

Integrating OneWorld Xe with MC/ServiceGuard provides redundancy and high availability for OneWorld Xe. This integration provides:

- minimal downtime in the event of a system failure
- automatic response to the user interface that owns running OneWorld batch jobs
- minimal delay before running OneWorld batch jobs are able to be restarted
- no reconfiguration of clients in a client/server environment; the ServiceGuard movement of the OneWorld server to another physical node is transparent to the client nodes.



In the first configuration tested, one primary node was used (stxhpcl1), with a second node initially not performing any OneWorld-related activity (stxhpcl2) (standby node). Both the active and standby nodes were connected to a High Availability Storage System (HASS) disk storage mechanism via FWD SCSI connection. The HASS contained the MC/ServiceGuard cluster lock disk, shared OneWorld Xe files and instance information needed by both the primary OneWorld node and the standby OneWorld node (upon a failover).

An additional node was part of this configuration. This node was configured as an Oracle Database Server. The Oracle Database has been previously certified as compatible with MC/ServiceGuard; thus, for this certification effort, it was decided that only OneWorld Xe would be configured in a failover architecture.

A remote node was connected via TCP/IP LAN to the same subnet as stxhpcl1 and stxhpcl2. This remote node, running Windows NT, was used to run the OneWorld Xe client software. This node was the source of client/server requests to the OneWorld Xe server, and was also used to submit batch jobs to the OneWorld Xe server.

Two different configurations were tested and certified:

Configuration #1 – A Single Instance of OneWorld Xe, running on one machine, with a dedicated standby machine.

- One package was created. This package mounted the shared volume group and file systems. The package then performed a set user (su) command, invoked the OneWorld environment, and ran the script to start OneWorld.

- A monitor script was written to monitor the jdenet_n and jdequeue processes. The script is run by MC/ServiceGuard during package start. The monitor script will stay in a loop, checking for the existence of these processes. If either or both of these processes do not exist, a failover scenario will be initiated.

- A HA Monitor was configured as part of the package, to monitor the available filesystem size of the OneWorld filesystems. This monitor was maintained by MC/ServiceGuard. If the available filesystem size dropped below 5% for any of the shared filesystems, MC/ServiceGuard would report this error, and initiate a failover scenario. This monitor was also configured as a package dependency, i.e. the package depended upon this filesystem resource to perform its work. If the filesystem resource was not available, the package would not start.

Configuration #2 – Two Instances of OneWorld Xe, each running on a separate machine, with each machine being able to failover to the other.

- Two packages were created, owpkg1 and owpkg2. Package owpkg1 is primary on node stxhpcl1 while package owpkg2 is primary on node stxhpcl2. Each package mounts a shared volume group and separate file system. Each package then performed a set user (su) command, invoked the OneWorld environment, and ran the script to start OneWorld.

- Once both packages had been started by MC/ServiceGuard, two separate and operational instances of OneWorld Xe were running. Each instance had its own IP address, own volume group and own file system. In actual operation, one OneWorld instance could have been used for interactive operation, while the other instance could have been used for batch operations.

- Each instance of OneWorld Xe accessed a common database owned by the Oracle Database Server, which was described earlier within this document.

- A monitor script was written to monitor the jdenet_n and jdequeue processes. The script is run by MC/ServiceGuard during package start. The monitor script will stay in a loop, checking for the existence of these processes. If either or both of these processes do not exist, a failover scenario for that package will be initiated.

- A HA Monitor was configured as part of the package, to monitor the available filesystem size of the OneWorld filesystems. This monitor was maintained by MC/ServiceGuard. If the available filesystem size on either machine dropped below 5% for any of the shared filesystems, MC/ServiceGuard would report this error, and initiate a failover scenario for that package. This monitor was also configured as a package dependency, i.e. the package depended upon this filesystem resource to perform its work. If the filesystem resource was not available, the package would not start.

The OneWorld Xe application is validated and certified by Hewlett-Packard as compatible with Hewlett-Packard's MC/ServiceGuard high availability software. OneWorld Xe can be monitored by MC/ServiceGuard, with the level of monitoring highly configurable and subject to the implementation plans of the customer.

This document details a set of tests showing that OneWorld Xe is compatible with MC/ServiceGuard. The tests show that if a node running a OneWorld Xe batch job fails, the job can be restarted on an alternate node in less than 30 seconds. Also, any client-server connections to failed OneWorld Xe processes can be reconnected to the OneWorld server running on an alternate node.

MC/ServiceGuard packages are dependent on having automated application startup and shutdown scripts. HP engineers have developed package configuration and control scripts that are suitable for use (after system-specific modification) in a OneWorld Xe production environment.

OneWorld Xe Implementation and Certification in an MC/ServiceGuard Cluster

The process followed for the certification of OneWorld Xe in an MC/ServiceGuard environment is detailed in:

Appendix 34: HP's Partner Technology Access Center High Availability Implementation and Certification Services Process and Methodology

Implementation and Certification Onsite Process Participants:

Hewlett-Packard: Walt Saiko (Partner Technology Access Center)
JD Edwards: Roger Miller (Server Technology)

MC/ServiceGuard Configuration

Configuration 1 – Single Instance of OneWorld Xe

Configuring the Cluster

Create the ASCII cluster template file

```
cmquerycl –v –C /etc/cmcluster/cluster1.ascii –n stxhpcl1 –n stxhpcl2
```

Modify the template (cluster1.ascii) to reflect the environment and to verify the cluster configuration.

```
cmcheckconf –v –C /etc/cmcluster/cmclconfig.ascii
```

Create the cluster by applying the configuration file. This will create the binary file "cmclconfig" and automatically distribute it among the nodes defined in the cluster.

```
cmapplyconf –v –C /etc/cmcluster/cmclconfig.ascii
```

Start the cluster and check the cluster status. Test the cluster halt also.

```
cmruncl –v –n stxhpcl1 –n stxhpcl2
cmviewcl –v
cmhaltcl –f –v
cmruncl –n stxhpcl1 –n stxhpcl2
```

Configuring a ServiceGuard Package on the Primary Node.

Create the package configuration files and tailor to the test environment. Do not include the second node at this stage.

```
cd /etc/cmcluster
mkdir owpkg
cmmakepkg –p owpkg.ascii          # Edit owpkg.ascii
```

Create package control scripts and tailor to the test environment. Do not include application startup/shutdown, service monitoring, or relocatable IP address at this stage.

```
cd owpkg
cmmakepkg –s control.sh
```

Shut down cluster, verify and distribute the binary configuration files

```
cmhaltcl –f –v
cmapplyconf –v –C /etc/cmcluster/cmclconfig.ascii –P owpkg.ascii
```

Test cluster and package startup. Unmount all logical volumes on shared volume group and deactivate the volume group

```
cmruncl                           # Start cluster and package
cmviewcl –v                       # Check that package has started
```

Add knowledge of the Secondary Node to the packages

```
edit owpkg.ascii
```

Shut down cluster, verify and distribute the binary configuration files

```
cmhaltcl –f –v
cmapplyconf –v –C /etc/cmcluster/cmclconfig.ascii –P owpkg.ascii
```

Test cluster and package startup.. Unmount all logical volumes on shared volume group and deactivate the volume group

```
cmruncl                           # Start cluster and package
cmviewcl –v                       # Check that package has started
```

Assign the dynamic IP address of the package.

```
Edit control.sh file to include dynamic IP address
cmhaltpkg owpkg
cmrunpkg –v owpkg
cmviewcl –v                          # Check package has started and dynamic IP
                                     # address is pingable
```

Enable the OneWorld Xe application to switch to a second node by editing the package control file

```
edit owpkg.ascii                     # add NODE_NAME stxhpcl2
cmapplyconf –v –C /etc/cmcluster/cmclconfig.ascii –P owpkg.ascii
cmhaltcl –f –v
cmruncl –v
```

Test package switching to stxhpcl2

```
cmhaltpkg owpkg                      # Halt package

cmmodpkg –e owpkg                    # Enable package switching

cmrunpkg -n stxhpcl2 owpkg
```

Add in OneWorld Xe startup/shutdown details to package control script (control.sh) and check successful package activation.

```
Edit control.sh file to include Oneworld Xe startup/shutdown
cmrunpkg –v owpkg
cmviewcl –v                          # Check package has started on node stxhpcl1
                                     # and OneWorld Xe binary is running
```

Test package switching to stxhpcl2

```
cmhaltpkg owpkg                      # Activate owpkg on stxhpcl2
cmmodpkg –e owpkg                    # verify OneWorld Xe binary running
cmrunpkg –n stxhpcl2 owpkg           # Enable package switching
```

Configuration 2 – Multiple Instances of OneWorld Xe

Configuring the Cluster

Create the ASCII cluster template file

```
cmquerycl –v –C /etc/cmcluster/cmclconfig.ascii –n stxhpcl1 –n stxhpcl2
```

Modify the template (cluster1.ascii) to reflect the environment and to verify the cluster configuration.

```
cmcheckconf –v –C /etc/cmcluster/cmclconfig.ascii
```

Create the cluster by applying the configuration file. This will create the binary file "cmclconfig" and automatically distribute it among the nodes defined in the cluster.

```
cmapplyconf –v –C /etc/cmcluster/cmclconfig.ascii
```

Start the cluster and check the cluster status. Test the cluster halt also.

```
cmruncl –v –n stxhpcl1 –n stxhpcl2
cmviewcl –v
cmhaltcl –f –v
cmruncl –n stxhpcl1 –n stxhpcl2
```

Configuring a ServiceGuard Package on Each Node.

Create the package configuration files and tailor to the test environment. Do not include the second node at this stage.

```
cd /etc/cmcluster
mkdir owpkg1
cmmakepkg –p owpkg.ascii        # Edit owpkg1.ascii
mkdir owpkg2
cmmakepkg -p owpkg2.ascii       # Edit owpkg2.ascii
```

Create package control scripts and tailor to the test environment. Do not include application startup/shutdown, service monitoring, or relocatable IP address at this stage.

```
cd owpkg1
cmmakepkg –s control.sh

cd ../owpkg2
cmmakepkg –s control.sh
```

Shut down cluster, verify and distribute the binary configuration files

```
cmhaltcl –f –v
cmapplyconf –v –C /etc/cmcluster/cmclconfig.ascii –P owpkg1.ascii -P owpkg2.ascii
```

Test cluster and package startup. Unmount all logical volumes on shared volume group and deactivate the volume groups

```
cmruncl                         # Start cluster and packages
cmviewcl –v                     # Check that packages have started
```

Add knowledge of the appropriate Secondary Node to the packages

```
edit owpkg1.ascii
edit owpkg2.ascii
```

Shut down cluster, verify and distribute the binary configuration files

```
cmhaltcl –f –v
cmapplyconf –v –C /etc/cmcluster/cmclconfig.ascii –P owpkg1.ascii -P owpkg2.ascii
```

Test cluster and package startup.. Unmount all logical volumes on shared volume groups and deactivate the volume groups

```
cmruncl                          # Start cluster and packages
cmviewcl –v                      # Check that packages have started
```

Assign the dynamic IP addresses of the packages.

```
Edit both control.sh  files to include dynamic IP addresses
cmrunpkg –v owpkg1
cmrunpkg –v owpkg2
cmviewcl –v                      # Check packages have started and dynamic IP
                                 # addresses are pingable
```

Enable the OneWorld Xe application to switch to a second node by editing the package control files

```
edit owpkg1.ascii                # add NODE_NAME stxhpcl2
edit owpkg2.ascii                # add NODE_NAME stxhpcl1
cmapplyconf –v –C /etc/cmcluster/cmclconfig.ascii –P owpkg1.ascii -P owpkg2.ascii
cmhaltcl –f –v
cmruncl –v
```

Test package switching to the alternate node

```
cmhaltpkg owpkg1                 # Halt packages
cmhaltpkg owpkg2

cmmodpkg –e owpkg1               # Enable package switching
cmmodpkg -e owpkg2

cmrunpkg -n stxhpcl2 owpkg1
cmrunpkg -n stxhpcl1 owpkg2
```

Add in OneWorld Xe startup/shutdown details to package control scripts (control.sh) and check successful package activation.

```
Edit control.sh files to include OneWorld Xe startup/shutdown
cmrunpkg –v owpkg1
cmrunpkg –v owpkg2
cmviewcl –v                      # Check packages have started and OneWorld
                                 # binaries are running
```

Test package switching to the alternate node

```
cmhaltpkg owpkg1                 # Activate owpkg1  & owpkg2
cmhaltpkg owpkg2                 # verify OW binaries running
cmmodpkg –e owpkg1               # Enable package switching
cmmodpkg -e owpkg2
cmrunpkg -n stxhpcl2 owpkg1
cmrunpkg -n stxhpcl1 owpkg2
```

Test Suite

Output of cmviewcl –v with the two servers, stxhpcl1 and stxhpcl2, up and running. This is the multiple instance configuration.

```
CLUSTER       STATUS
hpcluster     up

  NODE          STATUS       STATE
  stxhpcl1      up           running

    Network_Parameters:
    INTERFACE     STATUS       PATH         NAME
    PRIMARY       up           10/12/6      lan0

    PACKAGE       STATUS       STATE        PKG_SWITCH    NODE
    owpkg1        up           running      enabled       stxhpcl1

      Policy_Parameters:
      POLICY_NAME      CONFIGURED_VALUE
      Failover         configured_node
      Failback         manual

      Script_Parameters:
      ITEM       STATUS   MAX_RESTARTS  RESTARTS   NAME
      Service    up                  0         0   owmonitor
      Subnet     up                              10.225.69.0
      Resource   up                              /system/filesystem/availMb/tmp

      Node_Switching_Parameters:
      NODE_TYPE    STATUS       SWITCHING    NAME
      Primary      up           enabled      stxhpcl1      (current)
      Alternate    up           enabled      stxhpcl2

  NODE          STATUS       STATE
  stxhpcl2      up           running

    Network_Parameters:
    INTERFACE     STATUS       PATH         NAME
    PRIMARY       up           10/12/6      lan0

    PACKAGE       STATUS       STATE        PKG_SWITCH    NODE
    owpkg2        up           running      enabled       stxhpcl2

      Policy_Parameters:
      POLICY_NAME      CONFIGURED_VALUE
      Failover         configured_node
      Failback         manual

      Script_Parameters:
      ITEM       STATUS   MAX_RESTARTS  RESTARTS   NAME
      Service    up                  0         0   owmonitor2
      Subnet     up                              10.225.69.0

      Node_Switching_Parameters:
      NODE_TYPE    STATUS       SWITCHING    NAME
      Primary      up           enabled      stxhpcl2      (current)
      Alternate    up           enabled      stxhpcl1
```

Failover Test Scenarios

Test 1
Test package shutdown script execution.

Begin by bringing the packages UP on their Primary node. Use <ps -ef | grep jdenet> to verify that OW is up and running, and that the package IP addresses are pingable.

<cmhaltpkg> the OW packages. Check to confirm that the OW binaries are not running.

Test 2
Test package startup.

This test should be performed immediately following Test 1. With the OW packages down on their Primary nodes, start the packages using ServiceGuard command <cmrunpkg>, specifying that the packages should start on their Primary node.

Verify using <ps> that the OW processes are running. Interact with the processes using the client interface, and verify the results of the operation that is requested.

Test 3
Test local failure of LAN card in Primary machine to verify that the OW packages being tested use the standby LAN interface card when the Primary LAN interface card has failed.

Begin with the OW packages running on their Primary nodes. Disconnect each primary data LAN cable from designated ports on the network hub.

After a delay of several seconds, the LAN switch should occur. Verify that the OW packages (owpkg1 and owpkg2) are still pingable via their dynamic IP addresses, using the original Package IP addresses on the Standby Data LAN interface card.

Test 4
Restore LAN connectivity disconnected in Test 3, and confirm that switch back to the primary LAN occurs.

Begin by verifying that the OW packages are running on the Primary node.

After reconnecting the LAN cable of LAN0 to the hub, LAN contact to the package should hang for 1-2 seconds, until ServiceGuard has performed the LAN switch. After this time, confirm that LAN0 (Primary Data LAN) is now active once again.

Test 5
Test Powerfail switchover.

Begin with the OW packages running on their Primary nodes. Power off ONE of the Primary nodes by disconnecting the power cord from that node.

Verify the ServiceGuard package switch process occurs. The ServiceGuard Cluster Manager daemon should automatically recognize the loss of the Primary node heartbeat. The cluster reforms with the other healthy member, including the Secondary node for owpkg1 package. The cluster should free leftover holds on shared volume group(s) and the owpkg1 application should restart on the Secondary node.

Verify that the owpkg1 package is accessible via the client interface.

Note: when the Primary node is restarted, it will automatically rejoin the cluster, but it will not be enabled for package switching. No package switchback should occur at this time.

Test 6
Test the failover capability of a ServiceGuard-monitored OW application. In the owpkg1 package control script, monitor.sh is a service run by ServiceGuard It has a restart setting of 0. Confirm that when the monitor process is killed, a failover is initiated.

Begin with the OW packages being tested running on their primary nodes, under normal operating conditions.

Kill the monitor.sh process. Verify that ServiceGuard recognizes the loss of the monitored service, and initiates a failover.

Confirm that the OW package starts correctly on its Secondary node and that the OW binaries are running.

Test 7
Test the monitoring and exiting capability of the monitor.sh monitor process. Confirm that the monitor script is correctly monitoring all specified processes, and that failure of one of the monitored processes is reported. Failure of a monitored processed is reported by the monitor script returning an exit code of 1. This will initiate a ServiceGuard failover.

Begin with the OW packages operating under normal conditions on their primary nodes.

Find a monitored process using <ps -ef | grep jdenet> Terminate the process using the <kill -9 pid> command.

This will cause monitor.sh to return an exit code 1 to ServiceGuard. ServiceGuard will recognize that the service has exited with an error code, and perform a package halt on that node. ServiceGuard will then initiate a package failover to the Secondary node.

Confirm that the OW package starts correctly on the Secondary node, and that the OW package is accessible via the client interface.

Test 8
Test OW performance when the cluster heartbeat is totally lost.

For both the Primary and Secondary nodes for the packages, disconnect both primary and standby cluster heartbeat cables from the network hub. Altogether, four cables have been disconnected.

One and only one of the nodes should take control of the cluster lock disk and win the quorum.

If the Primary node takes control of the cluster lock disk: the owpkg1 package will continue running normally on the Primary node. The Secondary node will perform a TOC in order to avoid a potential race condition, and to remove locks held on the shared volume group used by owpkg2. The Primary node will take control of the shared volume group used by the owpkg2 package and start the owpkg2 package as if a normal failover had taken place. Package switching for both packages will be disabled since there is no other cluster member that can be contacted via network heartbeat

If the Secondary node takes control of the cluster lock disk: the owpkg2 package will continue running normally on the Secondary node. The Primary node will perform a TOC in order to avoid a potential race condition, and to remove locks held on the shared volume group used by owpkg1. The Secondary node will take control of the shared volume group used by the owpkg1 package and start the owpkg1 package as if a normal failover had taken place. Package switching for both packages will be disabled since there is no other cluster member who can be contacted via network heartbeat.

Through either path above, the OW packages should now be running on one of the cluster member.

Test 9

Test package failover when both the primary and standby LAN fail.

With the owpkg1 package running on its Primary node under normal conditions and under a typical workload, disconnect the Primary and Standby LAN on the Primary node.

Verify that the ServiceGuard Cluster Manager daemon recognizes loss of the data path. The cluster should reform with one healthy member, the Secondary node The primary node should free leftover holds on shared volume group(s). The owpkg1 package should start up correctly on its Secondary node.

Note: When the Primary node is reconnected, it will automatically rejoins the cluster, but is not enabled for package switching. No package switchback will occur at this time.

Appendix 1: OneWorld Xe cluster configuration file (cmclconfig.ascii)

```
# **********************************************************************
# ********* HIGH AVAILABILITY CLUSTER CONFIGURATION FILE ***************
# ***** For complete details about cluster parameters and how to     ****
# ***** set them, consult the cmquerycl(1m) manpage or your manual. ****
# **********************************************************************

# Enter a name for this cluster.  This name will be used to identify the
# cluster when viewing or manipulating it.

CLUSTER_NAME          hpcluster


# Cluster Lock Device Parameters.  This is the volume group that
# holds the cluster lock which is used to break a cluster formation
# tie.  This volume group should not be used by any other cluster
# as cluster lock device.

FIRST_CLUSTER_LOCK_VG         /dev/vgcl1


# Definition of nodes in the cluster.
# Repeat node definitions as necessary for additional nodes.

NODE_NAME             stxhpcl1
  NETWORK_INTERFACE   lan0
    HEARTBEAT_IP              10.225.69.20
  FIRST_CLUSTER_LOCK_PV       /dev/dsk/c0t1d0
# List of serial device file names
# For example:
# SERIAL_DEVICE_FILE  /dev/tty0p0

# Primary Network Interfaces on Bridged Net 1: lan0.
#   Warning: There are no standby network interfaces on bridged net 1.

NODE_NAME             stxhpcl2
  NETWORK_INTERFACE   lan0
    HEARTBEAT_IP              10.225.69.21
  FIRST_CLUSTER_LOCK_PV       /dev/dsk/c1t1d0
# List of serial device file names
# For example:
# SERIAL_DEVICE_FILE  /dev/tty0p0

# Primary Network Interfaces on Bridged Net 1: lan0.
#   Warning: There are no standby network interfaces on bridged net 1.


# Cluster Timing Parmeters (microseconds).

HEARTBEAT_INTERVAL            1000000
NODE_TIMEOUT          2000000


# Configuration/Reconfiguration Timing Parameters (microseconds).

AUTO_START_TIMEOUT    600000000
NETWORK_POLLING_INTERVAL      2000000

# Package Configuration Parameters.
# Enter the maximum number of packages which will be configured in the cluster.
# You can not add packages beyond this limit.
# This parameter is required.
MAX_CONFIGURED_PACKAGES               9


# List of cluster aware Volume Groups. These volume groups will
# be used by package applications via the vgchange -a e command.
```

```
# For example:
# VOLUME_GROUP          /dev/vgdatabase.
# VOLUME_GROUP          /dev/vg02.

VOLUME_GROUP            /dev/vgcl1
VOLUME_GROUP            /dev/vgcl2
```

Appendix 2: OneWorld Xe owpkg1 package configuration file (owpkg1.ascii)

```
# **********************************************************************
# ****** HIGH AVAILABILITY PACKAGE CONFIGURATION FILE (template) *******
# **********************************************************************
# ******* Note: This file MUST be edited before it can be used. ********
# * For complete details about package parameters and how to set them, *
# * consult the MC/ServiceGuard or ServiceGuard OPS Edition manpages   *
# * or manuals.                                                        *
# **********************************************************************

# Enter a name for this package.  This name will be used to identify the
# package when viewing or manipulating it.  It must be different from
# the other configured package names.

PACKAGE_NAME                    owpkg1


# Enter the failover policy for this package. This policy will be used
# to select an adoptive node whenever the package needs to be started.
# The default policy unless otherwise specified is CONFIGURED_NODE.
# This policy will select nodes in priority order from the list of
# NODE_NAME entries specified below.
#
# The alternative policy is MIN_PACKAGE_NODE. This policy will select
# the node, from the list of NODE_NAME entries below, which is
# running the least number of packages at the time this package needs
# to start.

FAILOVER_POLICY                         CONFIGURED_NODE


# Enter the failback policy for this package. This policy will be used
# to determine what action to take when a package is not running on
# its primary node and its primary node is capable of running the
# package. The default policy unless otherwise specified is MANUAL.
# The MANUAL policy means no attempt will be made to move the package
# back to its primary node when it is running on an adoptive node.
#
# The alternative policy is AUTOMATIC. This policy will attempt to
# move the package back to its primary node whenever the primary node
# is capable of running the package.

FAILBACK_POLICY                         MANUAL


# Enter the names of the nodes configured for this package.  Repeat
# this line as necessary for additional adoptive nodes.
# Order IS relevant.  Put the second Adoptive Node AFTER the first
# one.
# Example : NODE_NAME  original_node
#           NODE_NAME  adoptive_node

NODE_NAME                       stxhpcl1
NODE_NAME                       stxhpcl2


# Enter the complete path for the run and halt scripts.  In most cases
# the run script and halt script specified here will be the same script,
# the package control script generated by the cmmakepkg command.  This
# control script handles the run(ning) and halt(ing) of the package.
# If the script has not completed by the specified timeout value,
# it will be terminated.  The default for each script timeout is
# NO_TIMEOUT.  Adjust the timeouts as necessary to permit full
# execution of each script.
# Note: The HALT_SCRIPT_TIMEOUT should be greater than the sum of
# all SERVICE_HALT_TIMEOUT specified for all services.

RUN_SCRIPT                      /etc/cmcluster/owpkg1/control.sh
```

```
RUN_SCRIPT_TIMEOUT              NO_TIMEOUT
HALT_SCRIPT                     /etc/cmcluster/owpkg1/control.sh
HALT_SCRIPT_TIMEOUT             NO_TIMEOUT


# Enter the SERVICE_NAME, the SERVICE_FAIL_FAST_ENABLED and the
# SERVICE_HALT_TIMEOUT values for this package.  Repeat these
# three lines as necessary for additional service names.  All
# service names MUST correspond to the service names used by
# cmrunserv and cmhaltserv commands in the run and halt scripts.
#
# The value for SERVICE_FAIL_FAST_ENABLED can be either YES or
# NO.  If set to YES, in the event of a service failure, the
# cluster software will halt the node on which the service is
# running.  If SERVICE_FAIL_FAST_ENABLED is not specified, the
# default will be NO.
#
# SERVICE_HALT_TIMEOUT is represented in the number of seconds.
# This timeout is used to determine the length of time (in
# seconds) the cluster software will wait for the service to
# halt before a SIGKILL signal is sent to force the termination
# of the service.  In the event of a service halt, the cluster
# software will first send a SIGTERM signal to terminate the
# service.  If the service does not halt, after waiting for the
# specified SERVICE_HALT_TIMEOUT, the cluster software will send
# out the SIGKILL signal to the service to force its termination.
# This timeout value should be large enough to allow all cleanup
# processes associated with the service to complete.  If the
# SERVICE_HALT_TIMEOUT is not specified, a zero timeout will be
# assumed, meaning the cluster software will not wait at all
# before sending the SIGKILL signal to halt the service.
#
# Example: SERVICE_NAME                   DB_SERVICE
#          SERVICE_FAIL_FAST_ENABLED      NO
#          SERVICE_HALT_TIMEOUT           300
#
# To configure a service, uncomment the following lines and
# fill in the values for all of the keywords.
#
#SERVICE_NAME                   <service name>
#SERVICE_FAIL_FAST_ENABLED      <YES/NO>
#SERVICE_HALT_TIMEOUT           <number of seconds>

SERVICE_NAME                   owmonitor
SERVICE_FAIL_FAST_ENABLED      NO
SERVICE_HALT_TIMEOUT   100


# Enter the network subnet name that is to be monitored for this package.
# Repeat this line as necessary for additional subnet names.  If any of
# the subnets defined goes down, the package will be switched to another
# node that is configured for this package and has all the defined subnets
# available.

SUBNET                  10.225.69.0


# The keywords RESOURCE_NAME, RESOURCE_POLLING_INTERVAL,
# RESOURCE_START, and RESOURCE_UP_VALUE are used to specify Package
# Resource Dependencies.  To define a package Resource Dependency, a
# RESOURCE_NAME line with a fully qualified resource path name, and
# one or more RESOURCE_UP_VALUE lines are required.  The
# RESOURCE_POLLING_INTERVAL and the RESOURCE_START are optional.
#
# The RESOURCE_POLLING_INTERVAL indicates how often, in seconds, the
# resource is to be monitored.  It will be defaulted to 60 seconds if
# RESOURCE_POLLING_INTERVAL is not specified.
#
# The RESOURCE_START option can be set to either AUTOMATIC or DEFERRED.
# The default setting for RESOURCE_START is AUTOMATIC.  If AUTOMATIC
# is specified, ServiceGuard will start up resource monitoring for
```

```
# these AUTOMATIC resources automatically when the node starts up.
# If DEFERRED is selected, ServiceGuard will not attempt to start
# resource monitoring for these resources during node start up.  User
# should specify all the DEFERRED resources in the package run script
# so that these DEFERRED resources will be started up from the package
# run script during package run time.
#
# RESOURCE_UP_VALUE requires an operator and a value.  This defines
# the resource 'UP' condition.  The operators are =, !=, >, <, >=,
# and <=, depending on the type of value.  Values can be string or
# numeric.  If the type is string, then only = and != are valid
# operators.  If the string contains whitespace, it must be enclosed
# in quotes.  String values are case sensitive.  For example,
#
#                                   Resource is up when its value is
#                                   --------------------------------
#       RESOURCE_UP_VALUE     = UP                    "UP"
#       RESOURCE_UP_VALUE     != DOWN                 Any value except "DOWN"
#       RESOURCE_UP_VALUE     = "On Course"           "On Course"
#
# If the type is numeric, then it can specify a threshold, or a range to
# define a resource up condition.  If it is a threshold, then any operator
# may be used.  If a range is to be specified, then only > or >= may be used
# for the first operator, and only < or <= may be used for the second operator.
# For example,
#                                   Resource is up when its value is
#                                   --------------------------------
#       RESOURCE_UP_VALUE     = 5             5                     (threshold)
#       RESOURCE_UP_VALUE     > 5.1           greater than 5.1      (threshold)
#       RESOURCE_UP_VALUE     > -5 and < 10   between -5 and 10     (range)
#
# Note that "and" is required between the lower limit and upper limit
# when specifying a range.  The upper limit must be greater than the lower
# limit.  If RESOURCE_UP_VALUE is repeated within a RESOURCE_NAME block, then
# they are inclusively OR'd together.  Package Resource Dependencies may be
# defined by repeating the entire RESOURCE_NAME block.
#
# Example : RESOURCE_NAME               /net/interfaces/lan/status/lan0
#           RESOURCE_POLLING_INTERVAL 120
#           RESOURCE_START            AUTOMATIC
#           RESOURCE_UP_VALUE         = RUNNING
#           RESOURCE_UP_VALUE         = ONLINE
#
#           Means that the value of resource /net/interfaces/lan/status/lan0
#           will be checked every 120 seconds, and is considered to
#           be 'up' when its value is "RUNNING" or "ONLINE".
#
# Uncomment the following lines to specify Package Resource Dependencies.
#
#RESOURCE_NAME             <Full_path_name>
#RESOURCE_POLLING_INTERVAL  <numeric_seconds>
#RESOURCE_START             <AUTOMATIC/DEFERRED>
#RESOURCE_UP_VALUE         <op> <string_or_numeric> [and <op> <numeric>]
RESOURCE_NAME                 /system/filesystem/availMb/tmp
RESOURCE_POLLING_INTERVAL           60
RESOURCE_START                AUTOMATIC
RESOURCE_UP_VALUE >           50


# The default for PKG_SWITCHING_ENABLED is YES. In the event of a
# failure, this permits the cluster software to transfer the package
# to an adoptive node.  Adjust as necessary.

PKG_SWITCHING_ENABLED         YES


# The default for NET_SWITCHING_ENABLED is YES.  In the event of a
# failure, this permits the cluster software to switch LANs locally
# (transfer to a standby LAN card).  Adjust as necessary.

NET_SWITCHING_ENABLED         YES
```

```
# The default for NODE_FAIL_FAST_ENABLED is NO.  If set to YES,
# in the event of a failure, the cluster software will halt the node
# on which the package is running.  Adjust as necessary.

NODE_FAIL_FAST_ENABLED NO
```

Appendix 3: OneWorld Xe owpkg1 package control script (control.sh)

```
#"(#) A.11.09                                          $Date: 08/06/1999 $"
# **************************************************************************
# *                                                                        *
# *        HIGH AVAILABILITY PACKAGE CONTROL SCRIPT (template)             *
# *                                                                        *
# *                                                                        *
# **************************************************************************

# UNCOMMENT the variables as you set them.

# Set PATH to reference the appropriate directories.
PATH=/usr/bin:/usr/sbin:/etc:/bin

# VOLUME GROUP ACTIVATION:
# Specify the method of activation for volume groups.
# Leave the default ("VGCHANGE="vgchange -a e") if you want volume
# groups activated in exclusive mode. This assumes the volume groups have
# been initialized with 'vgchange -c y' at the time of creation.
#
# Uncomment the first line (VGCHANGE="vgchange -a e -q n"), and comment
# out the default, if your disks are mirrored on separate physical paths,
#
# Uncomment the second line (VGCHANGE="vgchange -a e -q n -s"), and comment
# out the default, if your disks are mirrored on separate physical paths,
# and you want the mirror resynchronization to ocurr in parallel with
# the package startup.
#
# Uncomment the third line (VGCHANGE="vgchange -a y") if you wish to
# use non-exclusive activation mode. Single node cluster configurations
# must use non-exclusive activation.
#
# VGCHANGE="vgchange -a e -q n"
# VGCHANGE="vgchange -a e -q n -s"
# VGCHANGE="vgchange -a y"
VGCHANGE="vgchange -a e"              # Default

# VOLUME GROUPS
# Specify which volume groups are used by this package. Uncomment VG[0]=""
# and fill in the name of your first volume group. You must begin with
# VG[0], and increment the list in sequence.
#
# For example, if this package uses your volume groups vg01 and vg02, enter:
#         VG[0]=vg01
#         VG[1]=vg02
#
# The volume group activation method is defined above. The filesystems
# associated with these volume groups are specified below.
#
VG[0]=/dev/vgcl1

# FILESYSTEMS
# Specify the filesystems which are used by this package. Uncomment
# LV[0]=""; FS[0]=""; FS_MOUNT_OPT[0]="" and fill in the name of your first
# logical volume, filesystem and mount option for the file system. You must
# begin with LV[0], FS[0] and FS_MOUNT_OPT[0] and increment the list in
# sequence.
#
# For example, if this package uses the file systems pkg1a and pkg1b,
# which are mounted on the logical volumes lvol1 and lvol2 with read and
# write options enter:
#         LV[0]=/dev/vg01/lvol1; FS[0]=/pkg1a; FS_MOUNT_OPT[0]="-o rw"
#         LV[1]=/dev/vg01/lvol2; FS[1]=/pkg1b; FS_MOUNT_OPT[1]="-o rw"
#
# The filesystems are defined as triplets of entries specifying the logical
# volume, the mount point and the mount options for the file system. Each
# filesystem will be fsck'd prior to being mounted. The filesystems will be
# mounted in the order specified during package startup and will be unmounted
```

```
# in reverse order during package shutdown. Ensure that volume groups
# referenced by the logical volume definitions below are included in
# volume group definitions above.
#
LV[0]=/dev/vgcl1/lv01; FS[0]=/u03; FS_MOUNT_OPT[0]=""

# FILESYSTEM UNMOUNT COUNT
# Specify the number of unmount attempts for each filesystem during package
# shutdown.  The default is set to 1.
FS_UMOUNT_COUNT=1

# IP ADDRESSES
# Specify the IP and Subnet address pairs which are used by this package.
# Uncomment IP[0]="" and SUBNET[0]="" and fill in the name of your first
# IP and subnet address. You must begin with IP[0] and SUBNET[0] and
# increment the list in sequence.
#
# For example, if this package uses an IP of 192.10.25.12 and a subnet of
# 192.10.25.0 enter:
#          IP[0]=192.10.25.12
#          SUBNET[0]=192.10.25.0 # (netmask=255.255.255.0)
#
# Hint: Run "netstat -i" to see the available subnets in the Network field.
#
# IP/Subnet address pairs for each IP address you want to add to a subnet
# interface card.  Must be set in pairs, even for IP addresses on the same
# subnet.
#
IP[0]=10.225.69.22
SUBNET[0]=10.225.69.0

# SERVICE NAMES AND COMMANDS.
# Specify the service name, command, and restart parameters which are
# used by this package. Uncomment SERVICE_NAME[0]="", SERVICE_CMD[0]="",
# SERVICE_RESTART[0]="" and fill in the name of the first service, command,
# and restart parameters. You must begin with SERVICE_NAME[0], SERVICE_CMD[0],
# and SERVICE_RESTART[0] and increment the list in sequence.
#
# For example:
#          SERVICE_NAME[0]=pkg1a
#          SERVICE_CMD[0]="/usr/bin/X11/xclock -display 192.10.25.54:0"
#          SERVICE_RESTART[0]=""  # Will not restart the service.
#
#          SERVICE_NAME[1]=pkg1b
#          SERVICE_CMD[1]="/usr/bin/X11/xload -display 192.10.25.54:0"
#          SERVICE_RESTART[1]="-r 2"   # Will restart the service twice.
#
#          SERVICE_NAME[2]=pkg1c
#          SERVICE_CMD[2]="/usr/sbin/ping"
#          SERVICE_RESTART[2]="-R" # Will restart the service an infinite
#                                  number of times.
#
# Note: No environmental variables will be passed to the command, this
# includes the PATH variable. Absolute path names are required for the
# service command definition.  Default shell is /usr/bin/sh.
#
SERVICE_NAME[0]=owmonitor
SERVICE_CMD[0]="/etc/cmcluster/owpkg1/monitor.sh"
SERVICE_RESTART[0]="-r 0"
#SERVICE_CMD[0]=""
#SERVICE_RESTART[0]=""

# DEFERRED_RESOURCE NAME
# Specify the full path name of the 'DEFERRED' resources configured for
# this package.  Uncomment DEFERRED_RESOURCE_NAME[0]="" and fill in the
# full path name of the resource.
#
#DEFERRED_RESOURCE_NAME[0]=""

# DTC manager information for each DTC.
# Example: DTC[0]=dtc_20
```

```
#DTC_NAME[0]=


# START OF CUSTOMER DEFINED FUNCTIONS

# This function is a place holder for customer define functions.
# You should define all actions you want to happen here, before the service is
# started.  You can create as many functions as you need.

function customer_defined_run_cmds
{
# ADD customer defined run commands.
: # do nothing instruction, because a function must contain some command.

       su oneworld <<EOF1
        . /u03/oneworld/b733_sp14/system/bin32/owenv
        /u03/oneworld/b733_sp14/system/bin32/RunOneWorld.sh
EOF1

       test_return 51
}

# This function is a place holder for customer define functions.
# You should define all actions you want to happen here, before the service is
# halted.

function customer_defined_halt_cmds
{
# ADD customer defined halt commands.
: # do nothing instruction, because a function must contain some command.
      su oneworld <<EOF2
        . /u03/oneworld/b733_sp14/system/bin32/owenv
        /u03/oneworld/b733_sp14/system/bin32/EndOneWorld.sh now
EOF2
       test_return 52
}

# END OF CUSTOMER DEFINED FUNCTIONS


# START OF RUN FUNCTIONS


function activate_volume_group
{
for I in ${VG[@]}
do
       if [[ "${VGCHANGE}" = "vgchange -a y" ]]
       then
              print "$(date '+%b %e %X') - Node \"$(hostname)\": Activating volume group $I
with non-exclusive option."
       else
              print "$(date '+%b %e %X') - \"$(hostname)\": Activating volume group $I with
exclusive option."
       fi

       $VGCHANGE $I
       test_return 1

       # If the -s option has been specified, then we perform
       # the resynchronization as a background task
       #
       if [[ ${VGCHANGE#*-s} != ${VGCHANGE} ]]
       then
           {
              if /sbin/vgsync $I
              then
                  print "$(date '+%b %e %X') - Node \"$(hostname)\": Resynchronized volume
group $I"
              else
```

```
                print "$(date '+%b %e %X') - Node \"$(hostname)\": Resynchronization of
volume group $I encountered an error"
            fi
        } &
    fi
done
}

# For each {file system/logical volume} pair, fsck the file system
# and mount it.  If the file system is busy, mounting of the file
# system will fail, the control script will exit with an error.

function check_and_mount
{
integer R=0

for I in ${LV[@]}
do
    if [[ $(mount -p | awk '$1 == "'$I'"') = "" ]]
    then
        RLV[$R]="${I%/*}/r${I##*/}"

        if [ -x /usr/sbin/fstyp ]
        then
                fstype[$R]=$(fstyp $I)
        fi
        (( R = $R + 1 ))
    fi
done

# Verify that there is at least one file system to check and what type.
if [[ ${RLV[@]} != "" ]]
then
    print -n "$(date '+%b %e %X') - Node \"$(hostname)\": "
    print "Checking filesystems:"
    print ${LV[@]} | tr ' ' '\012' | sed -e 's/^/   /'

    # If there is more than one filesystem type being checked
    # then each filesystem is check individually.
    #
    R=$(print ${fstype[*]} | tr ' ' '\012' | sort -u | wc -l)
    if (( R > 1 ))
    then
        R=0
        while (( R < ${#RLV[*]} ))
        do
            case ${fstype[$R]} in

                hfs)        fsck -F hfs -P ${RLV[$R]}
                            test_return 2
                            ;;

                vxfs)       fsck -F vxfs -y ${RLV[$R]}
                            test_return 2
                            ;;

                unk*)       fsck ${RLV[$R]}
                            test_return 2
                            ;;

                *)          if [[ ${fstype[$R]} = "" ]]
                            then
                                fsck ${RLV[$R]}
                            else
                                fsck -F ${fstype[$R]} ${RLV[$R]}
                            fi
                            test_return 2
                            ;;
            esac
            (( R = R + 1 ))
        done
```

```
        # If there is only one filesystem type being checked, then
        # multiple invocations of fsck can be avoided. All filesystems
        # are specified on the command line to one fsck invocation.
        #
        else
            case ${fstype} in

                hfs)    fsck -F hfs -P ${RLV[@]}
                        test_return 2
                        ;;

                vxfs)   fsck -F vxfs -y ${RLV[@]}
                        test_return 2
                        ;;

                unk*)   fsck ${RLV[@]}
                        test_return 2
                        ;;

                *)      if [[ ${fstype} = "" ]]
                        then
                            fsck ${RLV[@]}
                        else
                            fsck -F ${fstype} ${RLV[@]}
                        fi
                        test_return 2
                        ;;
            esac
        fi
fi

# Check exit value (set if any proceeding fsck calls failed)

if (( $exit_value == 1 ))
then
        deactivate_volume_group
        print "\n\t############ Node \"$(hostname)\": Package start failed  at $(date)
############"
        exit 1
fi

integer F=0
for I in ${LV[@]}
do
        if [[ $(mount | grep -e $I" ") = "" ]]
        then
                print "$(date '+%b %e %X') - Node \"$(hostname)\": Mounting $I at ${FS[$F]}"
                mount ${FS_MOUNT_OPT[$F]} $I ${FS[$F]}
                test_return 3
        else
                print "$(date '+%b %e %X') - Node \"$(hostname)\": WARNING:  File system
\"${FS[$F]}\" was already mounted."
        fi
        (( F = $F + 1 ))
done
}

# For each {IP address/subnet} pair, add the IP address to the subnet
# using cmmodnet(1m).

function add_ip_address
{
integer S=0
integer error=0

for I in ${IP[@]}
do
        print "$(date '+%b %e %X') - Node \"$(hostname)\": Adding IP address $I to subnet
${SUBNET[$S]}"
        XX=$( cmmodnet -a -i $I ${SUBNET[$S]} 2>&1 )
```

```
        if (( $? != 0 ))
        then
                if [[ $(echo $XX | grep "heartbeat IP") != "" ]]
                then
                        # IP has been configured as a heartbeat IP address.
                        print "$XX" >> $0.log
                        (( error = 1 ))
                else
                        YY=$( netstat -in | awk '$4 == "'${I}'"')
                        if [[ -z $YY ]]
                        then
                                print "$XX" >> $0.log
                                print "\tERROR:  Failed to add IP $I to subnet ${SUBNET[$S]}"
                                (( error = 1 ))
                        else
                                print "\tWARNING:  IP $I is already configured on the subnet
${SUBNET[$S]}"
                        fi
                fi
        fi
        (( S = $S + 1 ))
done

if (( error != 0 ))
then

# `let 0` is used to set the value of $? to 1. The function test_return
# requires $? to be set to 1 if it has to print error message.

        let 0
        test_return 4
fi

}

# Own and reset the DTC connections

function get_ownership_dtc
{
for I in ${DTC_NAME[@]}
do
        print "$(date '+%b %e %X') - Node \"$(hostname)\": Assigning Ownership of the DTC $I"
        dtcmodifyconfs -o $I
        test_return 5

        for J in ${IP[@]}
        do
                print "$(date '+%b %e %X') - Node \"$(hostname)\": Resetting the DTC
connections to IP address $J"
                dtcdiag -Q $J -q -f $I
                test_return 6
        done
done
}


# For each {service name/service command string} pair, start the
# service command string at the service name using cmrunserv(1m).

function start_services
{
integer C=0
for I in ${SERVICE_NAME[@]}
do
        print "$(date '+%b %e %X') - Node \"$(hostname)\": Starting service $I using"
        print "    \"${SERVICE_CMD[$C]}\""
             #
             # Check if cmrunserv should be called the old
             # way without a restart count.
             #
        if [[ "${SERVICE_RESTART[$C]}" = "" ]]
```

```
        then
            cmrunserv $I ">> $0.log 2>&1 ${SERVICE_CMD[$C]}"
        else
            cmrunserv ${SERVICE_RESTART[$C]} $I ">> $0.log 2>&1 ${SERVICE_CMD[$C]}"
        fi
        test_return 8
        (( C = $C + 1 ))
done
}


# For each {deferred resource name}, start resource monitoring for this
# resource using cmstartres(1m).

function start_resources
{
for I in ${DEFERRED_RESOURCE_NAME[@]}
do
        print "$(date '+%b %e %X') - Node \"$(hostname)\": Starting resource monitoring for
$I"
        cmstartres -u -p $PACKAGE $I >> $0.log 2>&1
        test_return 15
done
}

# END OF RUN FUNCTIONS.


# START OF HALT FUNCTIONS

# For each {deferred resource name}, stop resource monitoring for this
# resource using cmstopres(1m).

function stop_resources
{
for I in ${DEFERRED_RESOURCE_NAME[@]}
do
        print "$(date '+%b %e %X') - Node \"$(hostname)\": Stopping resource monitoring for
$I"
        cmstopres -p $PACKAGE $I >> $0.log 2>&1
        test_return 16
done
}


# Halt each service using cmhaltserv(1m).

function halt_services
{
for I in ${SERVICE_NAME[@]}
do
       print "$(date '+%b %e %X') - Node \"$(hostname)\": Halting service $I"
       cmhaltserv $I
       test_return 9
done
}

# Disown the DTC.

function disown_dtc
{
for I in ${DTC_NAME[@]}
do
       print "$(date '+%b %e %X') - Node \"$(hostname)\": Disowning the DTC $I"
       dtcmodifyconfs -d $I
       test_return 11
done
}

# For each IP address/subnet pair, remove the IP address from the subnet
```

```
# using cmmodnet(1m).

function remove_ip_address
{
integer S=0
integer error=0

for I in ${IP[@]}
do
        print "$(date '+%b %e %X') - Node \"$(hostname)\": Remove IP address $I from subnet
${SUBNET[$S]}"
        XX=$( cmmodnet -r -i $I ${SUBNET[$S]} 2>&1 )
        if (( $? != 0 ))
        then
                echo $XX | grep "is not configured on the subnet"
                if (( $? != 0 ))
                then
                        print "$XX" >> $0.log
                        (( error = 1 ))
                fi
        fi
        (( S = $S + 1 ))
done
if (( $error != 0 ))
then

# `let 0` is used to set the value of $? to 1. The function test_return
# requires $? to be set to 1 if it has to print error message.

        let 0
        test_return 12
fi
}

# Unmount each logical volume.

function umount_fs
{
integer UM_CNT=${FS_UMOUNT_COUNT:-1}

if [[ $UM_CNT < 1 ]]
then
   UM_CNT=1
fi

integer L=${#LV[*]}
while (( L > 0 ))
do
        (( L = L - 1 ))
        I=${LV[$L]}
        mount | grep -e $I" " > /dev/null 2>&1
        if (( $? == 0 ))
        then
                print "$(date '+%b %e %X') - Node \"$(hostname)\": Unmounting filesystem on
$I"
                print "\tWARNING:   Running fuser to remove anyone using the file system
directly."
                UM_COUNT=$UM_CNT
                while (( $UM_COUNT > 0 ))
                do
                fuser -ku $I
                umount $I
                if (( $? == 0 ))
                then
                        (( UM_COUNT = 0 ))
                else
                        if (( $UM_COUNT == 1 ))
                        then
                                let 0
                                test_return 13
                        fi
```

```
                        (( UM_COUNT = $UM_COUNT - 1 ))
                        sleep 1
                        if (( $UM_COUNT > 0 ))
                        then
                                print "\t$(date '+%b %e %X') - Unmount failed, trying again."
                        fi
                fi
                done
        fi
done
}


function deactivate_volume_group
{
for I in ${VG[@]}
do
        print "$(date '+%b %e %X') - Node \"$(hostname)\": Deactivating volume group $I"
        vgchange -a n $I
        test_return 14
done
}

# END OF HALT FUNCTIONS.

# FUNCTIONS COMMON TO BOTH RUN AND HALT.

# Test return value of functions and exit with NO RESTART if bad.
# Return value of 0 - 50 are reserved for use by Hewlett-Packard.
# System administrators can use numbers above 50 for return values.
        function test_return
        {
        if (( $? != 0 ))
        then
                case $1 in
                        1)
                        print "\tERROR:  Function activate_volume_group"
                        print "\tERROR:  Failed to activate $I"
                        deactivate_volume_group
                        exit 1
                        ;;

                        2)
                        print "\tERROR:  Function check_and_mount"
                        print "\tERROR:  Failed to fsck one of the logical volumes."
                        exit_value=1
                        ;;

                        3)
                        print "\tERROR:  Function check_and_mount"
                        print "\tERROR:  Failed to mount $I to ${FS[$F]}"
                        umount_fs
                        deactivate_volume_group
                        exit 1
                        ;;

                        4)
                        print "\tERROR:  Function add_ip_address"
                        print "\tERROR:  Failed to add IP address to subnet"
                        remove_ip_address
                        umount_fs
                        deactivate_volume_group
                        exit 1
                        ;;

                        5)
                        print "\tERROR:  Function get_ownership_dtc"
                        print "\tERROR:  Failed to own $I"
                        disown_dtc
                        remove_ip_address
                        umount_fs
```

```
deactivate_volume_group
exit 1
;;

6)
print "\tERROR:  Function get_ownership_dtc"
print "\tERROR:  Failed to switch $I"
disown_dtc
remove_ip_address
umount_fs
deactivate_volume_group
exit 1
;;

8)
print "\tERROR:  Function start_services"
print "\tERROR:  Failed to start service ${SERVICE_NAME[$C]}"
halt_services
customer_defined_halt_cmds
disown_dtc
remove_ip_address
umount_fs
deactivate_volume_group
exit 1
;;

9)
print "\tFunction halt_services"
print "\tWARNING: Failed to halt service $I"
;;

11)
print "\tERROR:  Function disown_dtc"
print "\tERROR:  Failed to disown $I from ${SUBNET[$S]}"
exit_value=1
;;

12)
print "\tERROR:  Function remove_ip_address"
print "\tERROR:  Failed to remove $I"
exit_value=1
;;

13)
print "\tERROR:  Function umount_fs"
print "\tERROR:  Failed to umount $I"
exit_value=1
;;

14)
print "\tERROR:  Function deactivate_volume_group"
print "\tERROR:  Failed to deactivate $I"
exit_value=1
;;

15)
print "\tERROR:  Function start_resources"
print "\tERROR:  Failed to start resource $I"
stop_resources
halt_services
customer_defined_halt_cmds
disown_dtc
remove_ip_address
umount_fs
deactivate_volume_group
exit 1
;;

16)
print "\tERROR:  Function stop_resources"
print "\tERROR:  Failed to stop resource $I"
```

```
                        exit_value=1
                        ;;

                        51)
                        print "\tERROR:  Function customer_defined_run_cmds"
                        print "\tERROR:  Failed to RUN customer commands"
                        halt_services
                        customer_defined_halt_cmds
                        disown_dtc
                        remove_ip_address
                        umount_fs
                        deactivate_volume_group
                        exit 1
                        ;;

                        52)
                        print "\tERROR:  Function customer_defined_halt_cmds"
                        print "\tERROR:  Failed to HALT customer commands"
                        exit_value=1
                        ;;

                        *)
                        print "\tERROR:  Failed, unknown error."
                        ;;
                esac
        fi
        }

        # END OF FUNCTIONS COMMON TO BOTH RUN AND HALT

        #-------------------MAINLINE Control Script Code Starts Here-----------------
        #
        # FUNCTION STARTUP SECTION.

        typeset MIN_VERSION="A.10.03"  # Minimum version this control script works on

        integer exit_value=0
        typeset CUR_VERSION

        #
        # Check that this control script is being run on a A.10.03 or later release
        # of MC/ServiceGuard or ServiceGuard OPS Edition.  The control scripts are forward
        # compatible but are not backward compatible because newer control
        # scripts use commands and option not available on older releases.

        CUR_VERSION="$(/usr/bin/what /usr/lbin/cmcld | /usr/bin/grep "Date" | \
                                /usr/bin/egrep '[AB]\...\...|NTT\...\...' | \
                                cut -f2 -d" ")"

        if [[ "${CUR_VERSION}" = ""  ]] || \
                                  [[ "${CUR_VERSION#*.}" < "${MIN_VERSION#*.}" ]]
        then
            print "ERROR:  Mismatched control script version ($MIN_VERSION).  You cannot run"
            print "\ta version ${MIN_VERSION} control_script on a node running pre"
            print "\t${MIN_VERSION} MC/ServiceGuard or ServiceGuard OPS Edition software"
            exit 1
        fi

        # Test to see if we are being called to run the package, or halt the package.

        if [[ $1 = "start" ]]
        then
                print "\n\t############ Node \"$(hostname)\": Starting package at $(date)
############"

                activate_volume_group

                check_and_mount

                add_ip_address
```

```
                get_ownership_dtc

                customer_defined_run_cmds

                start_services

                start_resources


        # Check exit value

                if (( $exit_value == 1 ))
                then
                        print "\n\t############ Node \"$(hostname)\": Package start failed  at
$(date) ############"
                        exit 1
                else
                        print "\n\t############ Node \"$(hostname)\": Package start completed
at $(date) ############"
                        exit 0
                fi

        elif [[ $1 = "stop" ]]
        then
                print "\n\t############ Node \"$(hostname)\": Halting package at $(date)
############"


                stop_resources

                halt_services

                customer_defined_halt_cmds

                disown_dtc

                remove_ip_address

                umount_fs

                deactivate_volume_group

        # Check exit value
                if (( $exit_value == 1 ))
                then
                        print "\n\t############ Node \"$(hostname)\": Package halt failed at
$(date) ############"
                        exit 1
                else
                        print "\n\t############ Node \"$(hostname)\": Package halt completed at
$(date) ############"
                        exit 0
                fi

fi
```

Appendix 4: OneWorld Xe owpkg2 package configuration file (owpkg2.ascii)

```
# **********************************************************************
# ****** HIGH AVAILABILITY PACKAGE CONFIGURATION FILE (template) *******
# **********************************************************************
# ******* Note: This file MUST be edited before it can be used. ********
# * For complete details about package parameters and how to set them, *
# * consult the MC/ServiceGuard or ServiceGuard OPS Edition manpages   *
# * or manuals.                                                        *
# **********************************************************************

# Enter a name for this package.  This name will be used to identify the
# package when viewing or manipulating it.  It must be different from
# the other configured package names.

PACKAGE_NAME                    owpkg2


# Enter the failover policy for this package. This policy will be used
# to select an adoptive node whenever the package needs to be started.
# The default policy unless otherwise specified is CONFIGURED_NODE.
# This policy will select nodes in priority order from the list of
# NODE_NAME entries specified below.
#
# The alternative policy is MIN_PACKAGE_NODE. This policy will select
# the node, from the list of NODE_NAME entries below, which is
# running the least number of packages at the time this package needs
# to start.

FAILOVER_POLICY                         CONFIGURED_NODE


# Enter the failback policy for this package. This policy will be used
# to determine what action to take when a package is not running on
# its primary node and its primary node is capable of running the
# package. The default policy unless otherwise specified is MANUAL.
# The MANUAL policy means no attempt will be made to move the package
# back to its primary node when it is running on an adoptive node.
#
# The alternative policy is AUTOMATIC. This policy will attempt to
# move the package back to its primary node whenever the primary node
# is capable of running the package.

FAILBACK_POLICY                         MANUAL


# Enter the names of the nodes configured for this package.  Repeat
# this line as necessary for additional adoptive nodes.
# Order IS relevant.  Put the second Adoptive Node AFTER the first
# one.
# Example : NODE_NAME  original_node
#           NODE_NAME  adoptive_node

NODE_NAME                       stxhpcl2
NODE_NAME                       stxhpcl1


# Enter the complete path for the run and halt scripts.  In most cases
# the run script and halt script specified here will be the same script,
# the package control script generated by the cmmakepkg command.  This
# control script handles the run(ning) and halt(ing) of the package.
# If the script has not completed by the specified timeout value,
# it will be terminated.  The default for each script timeout is
# NO_TIMEOUT.  Adjust the timeouts as necessary to permit full
# execution of each script.
# Note: The HALT_SCRIPT_TIMEOUT should be greater than the sum of
# all SERVICE_HALT_TIMEOUT specified for all services.

RUN_SCRIPT                      /etc/cmcluster/owpkg2/control.sh
RUN_SCRIPT_TIMEOUT              NO_TIMEOUT
```

```
HALT_SCRIPT                     /etc/cmcluster/owpkg2/control.sh
HALT_SCRIPT_TIMEOUT             NO_TIMEOUT


# Enter the SERVICE_NAME, the SERVICE_FAIL_FAST_ENABLED and the
# SERVICE_HALT_TIMEOUT values for this package.  Repeat these
# three lines as necessary for additional service names.  All
# service names MUST correspond to the service names used by
# cmrunserv and cmhaltserv commands in the run and halt scripts.
#
# The value for SERVICE_FAIL_FAST_ENABLED can be either YES or
# NO.  If set to YES, in the event of a service failure, the
# cluster software will halt the node on which the service is
# running.  If SERVICE_FAIL_FAST_ENABLED is not specified, the
# default will be NO.
#
# SERVICE_HALT_TIMEOUT is represented in the number of seconds.
# This timeout is used to determine the length of time (in
# seconds) the cluster software will wait for the service to
# halt before a SIGKILL signal is sent to force the termination
# of the service.  In the event of a service halt, the cluster
# software will first send a SIGTERM signal to terminate the
# service.  If the service does not halt, after waiting for the
# specified SERVICE_HALT_TIMEOUT, the cluster software will send
# out the SIGKILL signal to the service to force its termination.
# This timeout value should be large enough to allow all cleanup
# processes associated with the service to complete.  If the
# SERVICE_HALT_TIMEOUT is not specified, a zero timeout will be
# assumed, meaning the cluster software will not wait at all
# before sending the SIGKILL signal to halt the service.
#
# Example: SERVICE_NAME                   DB_SERVICE
#          SERVICE_FAIL_FAST_ENABLED      NO
#          SERVICE_HALT_TIMEOUT           300
#
# To configure a service, uncomment the following lines and
# fill in the values for all of the keywords.
#
#SERVICE_NAME                   <service name>
#SERVICE_FAIL_FAST_ENABLED      <YES/NO>
#SERVICE_HALT_TIMEOUT           <number of seconds>

SERVICE_NAME                    owmonitor2
SERVICE_FAIL_FAST_ENABLED       NO
SERVICE_HALT_TIMEOUT   100


# Enter the network subnet name that is to be monitored for this package.
# Repeat this line as necessary for additional subnet names.  If any of
# the subnets defined goes down, the package will be switched to another
# node that is configured for this package and has all the defined subnets
# available.

SUBNET                  10.225.69.0


# The keywords RESOURCE_NAME, RESOURCE_POLLING_INTERVAL,
# RESOURCE_START, and RESOURCE_UP_VALUE are used to specify Package
# Resource Dependencies.  To define a package Resource Dependency, a
# RESOURCE_NAME line with a fully qualified resource path name, and
# one or more RESOURCE_UP_VALUE lines are required.  The
# RESOURCE_POLLING_INTERVAL and the RESOURCE_START are optional.
#
# The RESOURCE_POLLING_INTERVAL indicates how often, in seconds, the
# resource is to be monitored.  It will be defaulted to 60 seconds if
# RESOURCE_POLLING_INTERVAL is not specified.
#
# The RESOURCE_START option can be set to either AUTOMATIC or DEFERRED.
# The default setting for RESOURCE_START is AUTOMATIC.  If AUTOMATIC
# is specified, ServiceGuard will start up resource monitoring for
# these AUTOMATIC resources automatically when the node starts up.
```

```
# If DEFERRED is selected, ServiceGuard will not attempt to start
# resource monitoring for these resources during node start up.  User
# should specify all the DEFERRED resources in the package run script
# so that these DEFERRED resources will be started up from the package
# run script during package run time.
#
# RESOURCE_UP_VALUE requires an operator and a value.  This defines
# the resource 'UP' condition.  The operators are =, !=, >, <, >=,
# and <=, depending on the type of value.  Values can be string or
# numeric.  If the type is string, then only = and != are valid
# operators.  If the string contains whitespace, it must be enclosed
# in quotes.  String values are case sensitive.  For example,
#
#                                    Resource is up when its value is
#                                    --------------------------------
#       RESOURCE_UP_VALUE      = UP                    "UP"
#       RESOURCE_UP_VALUE      != DOWN                 Any value except "DOWN"
#       RESOURCE_UP_VALUE      = "On Course"           "On Course"
#
# If the type is numeric, then it can specify a threshold, or a range to
# define a resource up condition.  If it is a threshold, then any operator
# may be used.  If a range is to be specified, then only > or >= may be used
# for the first operator, and only < or <= may be used for the second operator.
# For example,
#                                    Resource is up when its value is
#                                    --------------------------------
#       RESOURCE_UP_VALUE      = 5             5                    (threshold)
#       RESOURCE_UP_VALUE      > 5.1           greater than 5.1     (threshold)
#       RESOURCE_UP_VALUE      > -5 and < 10   between -5 and 10    (range)
#
# Note that "and" is required between the lower limit and upper limit
# when specifying a range.  The upper limit must be greater than the lower
# limit.  If RESOURCE_UP_VALUE is repeated within a RESOURCE_NAME block, then
# they are inclusively OR'd together.  Package Resource Dependencies may be
# defined by repeating the entire RESOURCE_NAME block.
#
# Example : RESOURCE_NAME               /net/interfaces/lan/status/lan0
#           RESOURCE_POLLING_INTERVAL 120
#           RESOURCE_START            AUTOMATIC
#           RESOURCE_UP_VALUE         = RUNNING
#           RESOURCE_UP_VALUE         = ONLINE
#
#           Means that the value of resource /net/interfaces/lan/status/lan0
#           will be checked every 120 seconds, and is considered to
#           be 'up' when its value is "RUNNING" or "ONLINE".
#
# Uncomment the following lines to specify Package Resource Dependencies.
#
#RESOURCE_NAME             <Full_path_name>
#RESOURCE_POLLING_INTERVAL  <numeric_seconds>
#RESOURCE_START             <AUTOMATIC/DEFERRED>
#RESOURCE_UP_VALUE         <op> <string_or_numeric> [and <op> <numeric>]


# The default for PKG_SWITCHING_ENABLED is YES. In the event of a
# failure, this permits the cluster software to transfer the package
# to an adoptive node.  Adjust as necessary.

PKG_SWITCHING_ENABLED          YES


# The default for NET_SWITCHING_ENABLED is YES.  In the event of a
# failure, this permits the cluster software to switch LANs locally
# (transfer to a standby LAN card).  Adjust as necessary.

NET_SWITCHING_ENABLED          YES


# The default for NODE_FAIL_FAST_ENABLED is NO.  If set to YES,
# in the event of a failure, the cluster software will halt the node
# on which the package is running.  Adjust as necessary.
```

```
NODE_FAIL_FAST_ENABLED NO
```

Appendix 5: OneWorld Xe owpkg2 package control file (control.sh)

```
#"(#) A.11.09                                          $Date: 08/06/1999 $"
# ************************************************************************
# *                                                                      *
# *        HIGH AVAILABILITY PACKAGE CONTROL SCRIPT (template)           *
# *                                                                      *
# *                                                                      *
# ************************************************************************

# UNCOMMENT the variables as you set them.

# Set PATH to reference the appropriate directories.
PATH=/usr/bin:/usr/sbin:/etc:/bin

# VOLUME GROUP ACTIVATION:
# Specify the method of activation for volume groups.
# Leave the default ("VGCHANGE="vgchange -a e") if you want volume
# groups activated in exclusive mode. This assumes the volume groups have
# been initialized with 'vgchange -c y' at the time of creation.
#
# Uncomment the first line (VGCHANGE="vgchange -a e -q n"), and comment
# out the default, if your disks are mirrored on separate physical paths,
#
# Uncomment the second line (VGCHANGE="vgchange -a e -q n -s"), and comment
# out the default, if your disks are mirrored on separate physical paths,
# and you want the mirror resynchronization to ocurr in parallel with
# the package startup.
#
# Uncomment the third line (VGCHANGE="vgchange -a y") if you wish to
# use non-exclusive activation mode. Single node cluster configurations
# must use non-exclusive activation.
#
# VGCHANGE="vgchange -a e -q n"
# VGCHANGE="vgchange -a e -q n -s"
# VGCHANGE="vgchange -a y"
VGCHANGE="vgchange -a e"             # Default

# VOLUME GROUPS
# Specify which volume groups are used by this package. Uncomment VG[0]=""
# and fill in the name of your first volume group. You must begin with
# VG[0], and increment the list in sequence.
#
# For example, if this package uses your volume groups vg01 and vg02, enter:
#         VG[0]=vg01
#         VG[1]=vg02
#
# The volume group activation method is defined above. The filesystems
# associated with these volume groups are specified below.
#
VG[0]=/dev/vgcl2

# FILESYSTEMS
# Specify the filesystems which are used by this package. Uncomment
# LV[0]=""; FS[0]=""; FS_MOUNT_OPT[0]="" and fill in the name of your first
# logical volume, filesystem and mount option for the file system. You must
# begin with LV[0], FS[0] and FS_MOUNT_OPT[0] and increment the list in
# sequence.
#
# For example, if this package uses the file systems pkg1a and pkg1b,
# which are mounted on the logical volumes lvol1 and lvol2 with read and
# write options enter:
#          LV[0]=/dev/vg01/lvol1; FS[0]=/pkg1a; FS_MOUNT_OPT[0]="-o rw"
#          LV[1]=/dev/vg01/lvol2; FS[1]=/pkg1b; FS_MOUNT_OPT[1]="-o rw"
#
# The filesystems are defined as triplets of entries specifying the logical
# volume, the mount point and the mount options for the file system. Each
# filesystem will be fsck'd prior to being mounted. The filesystems will be
# mounted in the order specified during package startup and will be unmounted
# in reverse order during package shutdown. Ensure that volume groups
```

```
# referenced by the logical volume definitions below are included in
# volume group definitions above.
#
LV[0]=/dev/vgcl2/lv01
FS[0]=/uo2
FS_MOUNT_OPT[0]=""

# FILESYSTEM UNMOUNT COUNT
# Specify the number of unmount attempts for each filesystem during package
# shutdown.  The default is set to 1.
FS_UMOUNT_COUNT=1

# IP ADDRESSES
# Specify the IP and Subnet address pairs which are used by this package.
# Uncomment IP[0]="" and SUBNET[0]="" and fill in the name of your first
# IP and subnet address. You must begin with IP[0] and SUBNET[0] and
# increment the list in sequence.
#
# For example, if this package uses an IP of 192.10.25.12 and a subnet of
# 192.10.25.0 enter:
#          IP[0]=192.10.25.12
#          SUBNET[0]=192.10.25.0 # (netmask=255.255.255.0)
#
# Hint: Run "netstat -i" to see the available subnets in the Network field.
#
# IP/Subnet address pairs for each IP address you want to add to a subnet
# interface card.  Must be set in pairs, even for IP addresses on the same
# subnet.
#
IP[0]=10.225.69.23
SUBNET[0]=10.225.69.0

# SERVICE NAMES AND COMMANDS.
# Specify the service name, command, and restart parameters which are
# used by this package. Uncomment SERVICE_NAME[0]="", SERVICE_CMD[0]="",
# SERVICE_RESTART[0]="" and fill in the name of the first service, command,
# and restart parameters. You must begin with SERVICE_NAME[0], SERVICE_CMD[0],
# and SERVICE_RESTART[0] and increment the list in sequence.
#
# For example:
#          SERVICE_NAME[0]=pkg1a
#          SERVICE_CMD[0]="/usr/bin/X11/xclock -display 192.10.25.54:0"
#          SERVICE_RESTART[0]=""  # Will not restart the service.
#
#          SERVICE_NAME[1]=pkg1b
#          SERVICE_CMD[1]="/usr/bin/X11/xload -display 192.10.25.54:0"
#          SERVICE_RESTART[1]="-r 2"   # Will restart the service twice.
#
#          SERVICE_NAME[2]=pkg1c
#          SERVICE_CMD[2]="/usr/sbin/ping"
#          SERVICE_RESTART[2]="-R" # Will restart the service an infinite
#                                  number of times.
#
# Note: No environmental variables will be passed to the command, this
# includes the PATH variable. Absolute path names are required for the
# service command definition.  Default shell is /usr/bin/sh.
#
SERVICE_NAME[0]=owmonitor2
SERVICE_CMD[0]="/etc/cmcluster/owpkg2/monitor.sh"
SERVICE_RESTART[0]="-r 0"
#SERVICE_CMD[0]=""
#SERVICE_RESTART[0]=""

# DEFERRED_RESOURCE NAME
# Specify the full path name of the 'DEFERRED' resources configured for
# this package.  Uncomment DEFERRED_RESOURCE_NAME[0]="" and fill in the
# full path name of the resource.
#
#DEFERRED_RESOURCE_NAME[0]=""

# DTC manager information for each DTC.
```

```
# Example: DTC[0]=dtc_20
#DTC_NAME[0]=


# START OF CUSTOMER DEFINED FUNCTIONS

# This function is a place holder for customer define functions.
# You should define all actions you want to happen here, before the service is
# started.  You can create as many functions as you need.

function customer_defined_run_cmds
{
# ADD customer defined run commands.
: # do nothing instruction, because a function must contain some command.

        su owuser1 <<EOF1
        . /u02/oneworld/b733_sp14/system/bin32/owenv
        /u02/oneworld/b733_sp14/system/bin32/RunOneWorld.sh
EOF1

       test_return 51
}

# This function is a place holder for customer define functions.
# You should define all actions you want to happen here, before the service is
# halted.

function customer_defined_halt_cmds
{
# ADD customer defined halt commands.
: # do nothing instruction, because a function must contain some command.

        su owuser1 <<EOF2
        . /u02/oneworld/b733_sp14/system/bin32/owenv
        /u02/oneworld/b733_sp14/system/bin32/EndOneWorld.sh now
EOF2

       test_return 52
}

# END OF CUSTOMER DEFINED FUNCTIONS


# START OF RUN FUNCTIONS


function activate_volume_group
{
for I in ${VG[@]}
do
       if [[ "${VGCHANGE}" = "vgchange -a y" ]]
       then
              print "$(date '+%b %e %X') - Node \"$(hostname)\": Activating volume group $I
with non-exclusive option."
       else
              print "$(date '+%b %e %X') - \"$(hostname)\": Activating volume group $I with
exclusive option."
       fi

       $VGCHANGE $I
       test_return 1

       # If the -s option has been specified, then we perform
       # the resynchronization as a background task
       #
       if [[ ${VGCHANGE#*-s} != ${VGCHANGE} ]]
       then
           {
              if /sbin/vgsync $I
              then
```

```
                print "$(date '+%b %e %X') - Node \"$(hostname)\": Resynchronized volume
group $I"
            else
                print "$(date '+%b %e %X') - Node \"$(hostname)\": Resynchronization of
volume group $I encountered an error"
            fi
        } &
    fi
done
}

# For each {file system/logical volume} pair, fsck the file system
# and mount it.  If the file system is busy, mounting of the file
# system will fail, the control script will exit with an error.

function check_and_mount
{
integer R=0

for I in ${LV[@]}
do
    if [[ $(mount -p | awk '$1 == "'$I'"') = "" ]]
    then
        RLV[$R]="${I%/*}/r${I##*/}"

        if [ -x /usr/sbin/fstyp ]
        then
                fstype[$R]=$(fstyp $I)
        fi
        (( R = $R + 1 ))
    fi
done

# Verify that there is at least one file system to check and what type.
if [[ ${RLV[@]} != "" ]]
then
    print -n "$(date '+%b %e %X') - Node \"$(hostname)\": "
    print "Checking filesystems:"
    print ${LV[@]} | tr ' ' '\012' | sed -e 's/^/   /'

    # If there is more than one filesystem type being checked
    # then each filesystem is check individually.
    #
    R=$(print ${fstype[*]} | tr ' ' '\012' | sort -u | wc -l)
    if (( R > 1 ))
    then
        R=0
        while (( R < ${#RLV[*]} ))
        do
            case ${fstype[$R]} in

                hfs)    fsck -F hfs -P ${RLV[$R]}
                        test_return 2
                        ;;

                vxfs)   fsck -F vxfs -y ${RLV[$R]}
                        test_return 2
                        ;;

                unk*)   fsck ${RLV[$R]}
                        test_return 2
                        ;;

                *)      if [[ ${fstype[$R]} = "" ]]
                        then
                            fsck ${RLV[$R]}
                        else
                            fsck -F ${fstype[$R]} ${RLV[$R]}
                        fi
                        test_return 2
                        ;;
```

```
                esac
                (( R = R + 1 ))
            done

        # If there is only one filesystem type being checked, then
        # multiple invocations of fsck can be avoided. All filesystems
        # are specified on the command line to one fsck invocation.
        #
        else
            case ${fstype} in

                hfs)    fsck -F hfs -P ${RLV[@]}
                        test_return 2
                        ;;

                vxfs)   fsck -F vxfs -y ${RLV[@]}
                        test_return 2
                        ;;

                unk*)   fsck ${RLV[@]}
                        test_return 2
                        ;;

                *)      if [[ ${fstype} = "" ]]
                        then
                            fsck ${RLV[@]}
                        else
                            fsck -F ${fstype} ${RLV[@]}
                        fi
                        test_return 2
                        ;;
            esac
        fi
fi

# Check exit value (set if any proceeding fsck calls failed)

if (( $exit_value == 1 ))
then
        deactivate_volume_group
        print "\n\t############ Node \"$(hostname)\": Package start failed  at $(date)
############"
        exit 1
fi

integer F=0
for I in ${LV[@]}
do
        if [[ $(mount | grep -e $I" ") = "" ]]
        then
                print "$(date '+%b %e %X') - Node \"$(hostname)\": Mounting $I at ${FS[$F]}"
                mount ${FS_MOUNT_OPT[$F]} $I ${FS[$F]}
                test_return 3
        else
                print "$(date '+%b %e %X') - Node \"$(hostname)\": WARNING:  File system
\"${FS[$F]}\" was already mounted."
        fi
        (( F = $F + 1 ))
done
}

# For each {IP address/subnet} pair, add the IP address to the subnet
# using cmmodnet(1m).

function add_ip_address
{
integer S=0
integer error=0

for I in ${IP[@]}
do
```

```
        print "$(date '+%b %e %X') - Node \"$(hostname)\": Adding IP address $I to subnet
${SUBNET[$S]}"
        XX=$( cmmodnet -a -i $I ${SUBNET[$S]} 2>&1 )
        if (( $? != 0 ))
        then
                if [[ $(echo $XX | grep "heartbeat IP") != "" ]]
                then
                        # IP has been configured as a heartbeat IP address.
                        print "$XX" >> $0.log
                        (( error = 1 ))
                else
                        YY=$( netstat -in | awk '$4 == "'${I}'"')
                        if [[ -z $YY ]]
                        then
                                print "$XX" >> $0.log
                                print "\tERROR:  Failed to add IP $I to subnet ${SUBNET[$S]}"
                                (( error = 1 ))
                        else
                                print "\tWARNING:  IP $I is already configured on the subnet
${SUBNET[$S]}"
                        fi
                fi
        fi
        (( S = $S + 1 ))
done

if (( error != 0 ))
then

# `let 0` is used to set the value of $? to 1. The function test_return
# requires $? to be set to 1 if it has to print error message.

        let 0
        test_return 4
fi

}

# Own and reset the DTC connections

function get_ownership_dtc
{
for I in ${DTC_NAME[@]}
do
        print "$(date '+%b %e %X') - Node \"$(hostname)\": Assigning Ownership of the DTC $I"
        dtcmodifyconfs -o $I
        test_return 5

        for J in ${IP[@]}
        do
                print "$(date '+%b %e %X') - Node \"$(hostname)\": Resetting the DTC
connections to IP address $J"
                dtcdiag -Q $J -q -f $I
                test_return 6
        done
done
}


# For each {service name/service command string} pair, start the
# service command string at the service name using cmrunserv(1m).

function start_services
{
integer C=0
for I in ${SERVICE_NAME[@]}
do
        print "$(date '+%b %e %X') - Node \"$(hostname)\": Starting service $I using"
        print "    \"${SERVICE_CMD[$C]}\""
             #
             # Check if cmrunserv should be called the old
```

```
            # way without a restart count.
            #
        if [[ "${SERVICE_RESTART[$C]}" = "" ]]
        then
            cmrunserv $I ">> $0.log 2>&1 ${SERVICE_CMD[$C]}"
        else
            cmrunserv ${SERVICE_RESTART[$C]} $I ">> $0.log 2>&1 ${SERVICE_CMD[$C]}"
        fi
        test_return 8
        (( C = $C + 1 ))
done
}


# For each {deferred resource name}, start resource monitoring for this
# resource using cmstartres(1m).

function start_resources
{
for I in ${DEFERRED_RESOURCE_NAME[@]}
do
        print "$(date '+%b %e %X') - Node \"$(hostname)\": Starting resource monitoring for
$I"
        cmstartres -u -p $PACKAGE $I >> $0.log 2>&1
        test_return 15
done
}

# END OF RUN FUNCTIONS.


# START OF HALT FUNCTIONS

# For each {deferred resource name}, stop resource monitoring for this
# resource using cmstopres(1m).

function stop_resources
{
for I in ${DEFERRED_RESOURCE_NAME[@]}
do
        print "$(date '+%b %e %X') - Node \"$(hostname)\": Stopping resource monitoring for
$I"
        cmstopres -p $PACKAGE $I >> $0.log 2>&1
        test_return 16
done
}


# Halt each service using cmhaltserv(1m).

function halt_services
{
for I in ${SERVICE_NAME[@]}
do
       print "$(date '+%b %e %X') - Node \"$(hostname)\": Halting service $I"
       cmhaltserv $I
       test_return 9
done
}

# Disown the DTC.

function disown_dtc
{
for I in ${DTC_NAME[@]}
do
       print "$(date '+%b %e %X') - Node \"$(hostname)\": Disowning the DTC $I"
       dtcmodifyconfs -d $I
       test_return 11
done
```

```
}

# For each IP address/subnet pair, remove the IP address from the subnet
# using cmmodnet(1m).

function remove_ip_address
{
integer S=0
integer error=0

for I in ${IP[@]}
do
        print "$(date '+%b %e %X') - Node \"$(hostname)\": Remove IP address $I from subnet
${SUBNET[$S]}"
        XX=$( cmmodnet -r -i $I ${SUBNET[$S]} 2>&1 )
        if (( $? != 0 ))
        then
                echo $XX | grep "is not configured on the subnet"
                if (( $? != 0 ))
                then
                        print "$XX" >> $0.log
                        (( error = 1 ))
                fi
        fi
        (( S = $S + 1 ))
done
if (( $error != 0 ))
then

# `let 0` is used to set the value of $? to 1. The function test_return
# requires $? to be set to 1 if it has to print error message.

        let 0
        test_return 12
fi
}

# Unmount each logical volume.

function umount_fs
{
integer UM_CNT=${FS_UMOUNT_COUNT:-1}

if [[ $UM_CNT < 1 ]]
then
   UM_CNT=1
fi

integer L=${#LV[*]}
while (( L > 0 ))
do
        (( L = L - 1 ))
        I=${LV[$L]}
        mount | grep -e $I" " > /dev/null 2>&1
        if (( $? == 0 ))
        then
                print "$(date '+%b %e %X') - Node \"$(hostname)\": Unmounting filesystem on
$I"
                print "\tWARNING:   Running fuser to remove anyone using the file system
directly."
                UM_COUNT=$UM_CNT
                while (( $UM_COUNT > 0 ))
                do
                fuser -ku $I
                umount $I
                if (( $? == 0 ))
                then
                        (( UM_COUNT = 0 ))
                else
                        if (( $UM_COUNT == 1 ))
                        then
```

```
                        let 0
                        test_return 13
                fi
                (( UM_COUNT = $UM_COUNT - 1 ))
                sleep 1
                if (( $UM_COUNT > 0 ))
                then
                        print "\t$(date '+%b %e %X') - Unmount failed, trying again."
                fi
        fi
        done
    fi
done
}


function deactivate_volume_group
{
for I in ${VG[@]}
do
    print "$(date '+%b %e %X') - Node \"$(hostname)\": Deactivating volume group $I"
    vgchange -a n $I
    test_return 14
done
}

# END OF HALT FUNCTIONS.

# FUNCTIONS COMMON TO BOTH RUN AND HALT.

# Test return value of functions and exit with NO RESTART if bad.
# Return values of 0 - 50 are reserved for use by Hewlett-Packard.
# System administrators can use numbers above 50 for return values.
    function test_return
    {
    if (( $? != 0 ))
    then
        case $1 in
            1)
            print "\tERROR:  Function activate_volume_group"
            print "\tERROR:  Failed to activate $I"
            deactivate_volume_group
            exit 1
            ;;

            2)
            print "\tERROR:  Function check_and_mount"
            print "\tERROR:  Failed to fsck one of the logical volumes."
            exit_value=1
            ;;

            3)
            print "\tERROR:  Function check_and_mount"
            print "\tERROR:  Failed to mount $I to ${FS[$F]}"
            umount_fs
            deactivate_volume_group
            exit 1
            ;;

            4)
            print "\tERROR:  Function add_ip_address"
            print "\tERROR:  Failed to add IP address to subnet"
            remove_ip_address
            umount_fs
            deactivate_volume_group
            exit 1
            ;;

            5)
            print "\tERROR:  Function get_ownership_dtc"
            print "\tERROR:  Failed to own $I"
```

```
disown_dtc
remove_ip_address
umount_fs
deactivate_volume_group
exit 1
;;

6)
print "\tERROR:  Function get_ownership_dtc"
print "\tERROR:  Failed to switch $I"
disown_dtc
remove_ip_address
umount_fs
deactivate_volume_group
exit 1
;;

8)
print "\tERROR:  Function start_services"
print "\tERROR:  Failed to start service ${SERVICE_NAME[$C]}"
halt_services
customer_defined_halt_cmds
disown_dtc
remove_ip_address
umount_fs
deactivate_volume_group
exit 1
;;

9)
print "\tFunction halt_services"
print "\tWARNING: Failed to halt service $I"
;;

11)
print "\tERROR:  Function disown_dtc"
print "\tERROR:  Failed to disown $I from ${SUBNET[$S]}"
exit_value=1
;;

12)
print "\tERROR:  Function remove_ip_address"
print "\tERROR:  Failed to remove $I"
exit_value=1
;;

13)
print "\tERROR:  Function umount_fs"
print "\tERROR:  Failed to unmount $I"
exit_value=1
;;

14)
print "\tERROR:  Function deactivate_volume_group"
print "\tERROR:  Failed to deactivate $I"
exit_value=1
;;

15)
print "\tERROR:  Function start_resources"
print "\tERROR:  Failed to start resource $I"
stop_resources
halt_services
customer_defined_halt_cmds
disown_dtc
remove_ip_address
umount_fs
deactivate_volume_group
exit 1
;;
```

```
                        16)
                        print "\tERROR:  Function stop_resources"
                        print "\tERROR:  Failed to stop resource $I"
                        exit_value=1
                        ;;

                        51)
                        print "\tERROR:  Function customer_defined_run_cmds"
                        print "\tERROR:  Failed to RUN customer commands"
                        halt_services
                        customer_defined_halt_cmds
                        disown_dtc
                        remove_ip_address
                        umount_fs
                        deactivate_volume_group
                        exit 1
                        ;;

                        52)
                        print "\tERROR:  Function customer_defined_halt_cmds"
                        print "\tERROR:  Failed to HALT customer commands"
                        exit_value=1
                        ;;

                        *)
                        print "\tERROR:  Failed, unknown error."
                        ;;
                esac
        fi
        }

        # END OF FUNCTIONS COMMON TO BOTH RUN AND HALT

        #-------------------MAINLINE Control Script Code Starts Here-----------------
        #
        # FUNCTION STARTUP SECTION.

        typeset MIN_VERSION="A.10.03"  # Minimum version this control script works on

        integer exit_value=0
        typeset CUR_VERSION

        #
        # Check that this control script is being run on a A.10.03 or later release
        # of MC/ServiceGuard or ServiceGuard OPS Edition.  The control scripts are forward
        # compatible but are not backward compatible because newer control
        # scripts use commands and option not available on older releases.

        CUR_VERSION="$(/usr/bin/what /usr/lbin/cmcld | /usr/bin/grep "Date" | \
                                /usr/bin/egrep '[AB]\...\...|NTT\...\...' | \
                                cut -f2 -d" ")"

        if [[ "${CUR_VERSION}" = ""  ]] || \
                                [[ "${CUR_VERSION#*.}" < "${MIN_VERSION#*.}" ]]
        then
            print "ERROR:  Mismatched control script version ($MIN_VERSION).  You cannot run"
            print "\ta version ${MIN_VERSION} control_script on a node running pre"
            print "\t${MIN_VERSION} MC/ServiceGuard or ServiceGuard OPS Edition software"
            exit 1
        fi

        # Test to see if we are being called to run the package, or halt the package.

        if [[ $1 = "start" ]]
        then
                print "\n\t############ Node \"$(hostname)\": Starting package at $(date)
############"

                activate_volume_group

                check_and_mount
```

```
                add_ip_address

                get_ownership_dtc

                customer_defined_run_cmds

                start_services

                start_resources


        # Check exit value

                if (( $exit_value == 1 ))
                then
                        print "\n\t############ Node \"$(hostname)\": Package start failed  at
$(date) ############"
                        exit 1
                else
                        print "\n\t############ Node \"$(hostname)\": Package start completed
at $(date) ############"
                        exit 0
                fi

        elif [[ $1 = "stop" ]]
        then
                print "\n\t############ Node \"$(hostname)\": Halting package at $(date)
############"


                stop_resources

                halt_services

                customer_defined_halt_cmds

                disown_dtc

                remove_ip_address

                umount_fs

                deactivate_volume_group

        # Check exit value
                if (( $exit_value == 1 ))
                then
                        print "\n\t############ Node \"$(hostname)\": Package halt failed at
$(date) ############"
                        exit 1
                else
                        print "\n\t############ Node \"$(hostname)\": Package halt completed at
$(date) ############"
                        exit 0
                fi

fi
```

Appendix 6: OneWorld Xe Monitor Script (monitor.sh) (same script for each package)

```
#!/bin/ksh

sleep 30
USER="owuser1"
CHECKFOR="jdenet_n jdequeue"

trap "exit" 15

while true
do
        for i in $CHECKFOR
        do
                print ""
                print "checking for process $i"
                ps -ef | grep $i | grep $USER | grep -v grep > /dev/null 2>&1
                if [ $? -ne 0 ]
                then
                        print "\n"
                        print "exiting monitor script - process $i not found"
                        exit 1
                fi
        done
        sleep 15
done
```

Appendix 7: Output of <bdf> on node stxhpcl1

```
Filesystem          kbytes    used   avail %used Mounted on
/dev/vg00/lvol3     143360   28396  107830   21% /
/dev/vg00/lvol1      83733   27523   47836   37% /stand
/dev/vg00/lvol8     512000  304403  195643   61% /var
/dev/vg00/lvol7     512000  381535  122314   76% /usr
/dev/vg00/lvol4      65536    1130   60384    2% /tmp
/dev/vg00/lvol6     348160   63771  266678   19% /opt
/dev/vg00/lvol5      20480    1351   17988    7% /home
/dev/vg01/lv01     4096000 1238276 2679117   32% /u01
/dev/vgcl1/lv01   16384000 2111310 13826718   13% /u03
```

Appendix 8: Output of <bdf> on node stxhpcl2

```
Filesystem          kbytes    used   avail %used Mounted on
/dev/vg00/lvol3     143360   67656   71009   49% /
/dev/vg00/lvol1      83733   27523   47836   37% /stand
/dev/vg00/lvol8     512000  306623  193514   61% /var
/dev/vg00/lvol7     512000  381550  122299   76% /usr
/dev/vg00/lvol4      65536    1272   60314    2% /tmp
/dev/vg00/lvol6     348160  170584  166492   51% /opt
/dev/vg00/lvol5      20480    1348   17991    7% /home
/dev/vg01/lv01     4096000  447897 3420097   12% /u01
/dev/vgcl2/lv01   16384000 2903542 13059198   18% /u02
```

Appendix 9: Output of <cmviewcl -v>

```
CLUSTER       STATUS
hpcluster     up

  NODE          STATUS       STATE
  stxhpcl1      up           running

    Network_Parameters:
    INTERFACE     STATUS       PATH         NAME
    PRIMARY       up           10/12/6      lan0

    PACKAGE       STATUS       STATE        PKG_SWITCH    NODE
    owpkg1        up           running      enabled       stxhpcl1

      Policy_Parameters:
      POLICY_NAME      CONFIGURED_VALUE
      Failover         configured_node
      Failback         manual

      Script_Parameters:
      ITEM       STATUS   MAX_RESTARTS  RESTARTS   NAME
      Service    up                  0         0   owmonitor
      Subnet     up                              10.225.69.0
      Resource   up                              /system/filesystem/availMb/tmp

      Node_Switching_Parameters:
      NODE_TYPE     STATUS       SWITCHING     NAME
      Primary       up           enabled       stxhpcl1      (current)
      Alternate     up           enabled       stxhpcl2

  NODE          STATUS       STATE
  stxhpcl2      up           running

    Network_Parameters:
    INTERFACE     STATUS       PATH         NAME
    PRIMARY       up           10/12/6      lan0

    PACKAGE       STATUS       STATE        PKG_SWITCH    NODE
    owpkg2        up           running      enabled       stxhpcl2

      Policy_Parameters:
      POLICY_NAME      CONFIGURED_VALUE
      Failover         configured_node
      Failback         manual

      Script_Parameters:
      ITEM       STATUS   MAX_RESTARTS  RESTARTS   NAME
      Service    up                  0         0   owmonitor2
      Subnet     up                              10.225.69.0

      Node_Switching_Parameters:
      NODE_TYPE     STATUS       SWITCHING     NAME
      Primary       up           enabled       stxhpcl2      (current)
      Alternate     up           enabled       stxhpcl1
```

Appendix 10: Contents of /etc/fstab on node stxhpcl1

```
# System /etc/fstab file.  Static information about the file systems
# See fstab(4) and sam(1M) for further details on configuring devices.
/dev/vg00/lvol3 / vxfs delaylog 0 1
/dev/vg00/lvol1 /stand hfs defaults 0 1
/dev/vg00/lvol4 /tmp vxfs delaylog 0 2
/dev/vg00/lvol5 /home vxfs delaylog 0 2
/dev/vg00/lvol6 /opt vxfs delaylog 0 2
/dev/vg00/lvol7 /usr vxfs delaylog 0 2
/dev/vg00/lvol8 /var vxfs delaylog 0 2
#/dev/vgcl/lv01 /u01 vxfs rw,suid,nolargefiles,delaylog,datainlog 0 2
#/dev/vgcl/lv02 /u02 vxfs rw,suid,nolargefiles,delaylog,datainlog 0 2
#/dev/vgcl/lv03 /u03 vxfs rw,suid,nolargefiles,delaylog,datainlog 0 2
#/dev/vgcl/lv04 /u04 vxfs rw,suid,nolargefiles,delaylog,datainlog 0 2
/dev/vg01/lv01 /u01 vxfs rw,suid,nolargefiles,delaylog,datainlog 0 2
/dev/vgcl1/lv01 /u03 vxfs rw,suid,nolargefiles,delaylog,datainlog 0 2
```

Appendix 11: Contents of /etc/fstab on node stxhpcl2

```
# System /etc/fstab file.  Static information about the file systems
# See fstab(4) and sam(1M) for further details on configuring devices.
/dev/vg00/lvol3 / vxfs delaylog 0 1
/dev/vg00/lvol1 /stand hfs defaults 0 1
/dev/vg00/lvol4 /tmp vxfs delaylog 0 2
/dev/vg00/lvol5 /home vxfs delaylog 0 2
/dev/vg00/lvol6 /opt vxfs delaylog 0 2
/dev/vg00/lvol7 /usr vxfs delaylog 0 2
/dev/vg00/lvol8 /var vxfs delaylog 0 2
#/dev/vgcl/lv01 /u01 vxfs rw,suid,nolargefiles,delaylog,datainlog 0 2
#/dev/vgcl/lv02 /u02 vxfs rw,suid,nolargefiles,delaylog,datainlog 0 2
#/dev/vgcl/lv03 /u03 vxfs rw,suid,nolargefiles,delaylog,datainlog 0 2
#/dev/vgcl/lv04 /u04 vxfs rw,suid,nolargefiles,delaylog,datainlog 0 2
/dev/vg01/lv01 /u01 vxfs rw,suid,nolargefiles,delaylog,datainlog 0 2
/dev/vgcl2/lv01 /u02 vxfs rw,suid,nolargefiles,delaylog,datainlog 0 2
```

Appendix 12: Contents of /etc/hosts

```
# @(#)hosts $Revision: 1.9.214.1 $ $Date: 96/10/08 13:20:01 $
#
# The form for each entry is:
# <internet address>   <official hostname> <aliases>
#
# For example:
# 192.1.2.34   hpfcrm  loghost
#
# See the hosts(4) manual page for more information.
# Note: The entries cannot be preceded by a space.
#       The format described in this file is the correct format.
#       The original Berkeley manual page contains an error in
#       the format description.
#

10.225.69.20    stxhpcl1
127.0.0.1       localhost       loopback
10.225.69.21    stxhpcl2

10.225.69.22    hpcluster
10.225.69.23    hpcluster2

10.0.40.73      corowsn1
```

Appendix 13: Output of <ioscan -f>

```
Class        I  H/W Path     Driver       S/W State H/W Type  Description
=============================================================================
bc           0              root         CLAIMED   BUS_NEXUS
bc           1  8            ccio         CLAIMED   BUS_NEXUS I/O Adapter
bc           2  10           ccio         CLAIMED   BUS_NEXUS I/O Adapter
ext_bus      0  10/0         c720         CLAIMED   INTERFACE GSC built-in Fast/Wide SCSI
Interface
target       0  10/0.1        tgt          CLAIMED   DEVICE
disk         0  10/0.1.0      sdisk        CLAIMED   DEVICE    SEAGATE ST34371W
target       1  10/0.3        tgt          CLAIMED   DEVICE
disk         1  10/0.3.0      sdisk        CLAIMED   DEVICE    SEAGATE ST34371W
target       2  10/0.4        tgt          CLAIMED   DEVICE
disk         2  10/0.4.0      sdisk        CLAIMED   DEVICE    SEAGATE ST34371W
target       3  10/0.5        tgt          CLAIMED   DEVICE
disk         3  10/0.5.0      sdisk        CLAIMED   DEVICE    SEAGATE ST34371W
target       4  10/0.6        tgt          CLAIMED   DEVICE
disk         4  10/0.6.0      sdisk        CLAIMED   DEVICE    SEAGATE ST34371W
target       5  10/0.7        tgt          CLAIMED   DEVICE
ctl          0  10/0.7.0      sctl         CLAIMED   DEVICE    Initiator
target       6  10/0.9        tgt          CLAIMED   DEVICE
disk         5  10/0.9.0      sdisk        CLAIMED   DEVICE    SEAGATE ST34371W
target       7  10/0.10       tgt          CLAIMED   DEVICE
disk         6  10/0.10.0     sdisk        CLAIMED   DEVICE    SEAGATE ST34371W
target       8  10/0.11       tgt          CLAIMED   DEVICE
disk         7  10/0.11.0     sdisk        CLAIMED   DEVICE    SEAGATE ST34371W
bc           3  10/4          bc           CLAIMED   BUS_NEXUS Bus Converter
tty          0  10/4/0        mux2         CLAIMED   INTERFACE MUX
ext_bus      1  10/8          c720         CLAIMED   INTERFACE GSC add-on Fast/Wide SCSI
Interface
target       9  10/8.0        tgt          CLAIMED   DEVICE
disk         8  10/8.0.0      sdisk        CLAIMED   DEVICE    SEAGATE ST34371W
target      10  10/8.3        tgt          CLAIMED   DEVICE
disk         9  10/8.3.0      sdisk        CLAIMED   DEVICE    SEAGATE ST34371W
target      11  10/8.4        tgt          CLAIMED   DEVICE
disk        10  10/8.4.0      sdisk        CLAIMED   DEVICE    SEAGATE ST34371W
target      12  10/8.5        tgt          CLAIMED   DEVICE
disk        11  10/8.5.0      sdisk        CLAIMED   DEVICE    SEAGATE ST34371W
target      13  10/8.6        tgt          CLAIMED   DEVICE
disk        12  10/8.6.0      sdisk        CLAIMED   DEVICE    SEAGATE ST34371W
target      14  10/8.12       tgt          CLAIMED   DEVICE
disk        13  10/8.12.0     sdisk        CLAIMED   DEVICE    SEAGATE ST34371W
target      15  10/8.13       tgt          CLAIMED   DEVICE
disk        14  10/8.13.0     sdisk        CLAIMED   DEVICE    SEAGATE ST34371W
target      16  10/8.14       tgt          CLAIMED   DEVICE
disk        15  10/8.14.0     sdisk        CLAIMED   DEVICE    SEAGATE ST34371W
target      17  10/8.15       tgt          CLAIMED   DEVICE
ctl          1  10/8.15.0     sctl         CLAIMED   DEVICE    Initiator
ba           0  10/12         bus_adapter  CLAIMED   BUS_NEXUS Core I/O Adapter
ext_bus      3  10/12/0       CentIf       CLAIMED   INTERFACE Built-in Parallel Interface
ext_bus      2  10/12/5       c720         CLAIMED   INTERFACE Built-in SCSI
target      18  10/12/5.0     tgt          CLAIMED   DEVICE
tape         0  10/12/5.0.0   stape        CLAIMED   DEVICE    HP      C1533A
target      19  10/12/5.2     tgt          CLAIMED   DEVICE
disk        16  10/12/5.2.0   sdisk        CLAIMED   DEVICE    TOSHIBA CD-ROM XM-5701TA
target      20  10/12/5.7     tgt          CLAIMED   DEVICE
ctl          2  10/12/5.7.0   sctl         CLAIMED   DEVICE    Initiator
lan          0  10/12/6       lan2         CLAIMED   INTERFACE Built-in LAN
ps2          0  10/12/7       ps2          CLAIMED   INTERFACE Built-in Keyboard/Mouse
processor    0  32            processor    CLAIMED   PROCESSOR Processor
processor    1  34            processor    CLAIMED   PROCESSOR Processor
memory       0  49            memory       CLAIMED   MEMORY    Memory
```

Appendix 14: Output of <lanscan>

```
Hardware Station         Crd Hdw   Net-Interface  NM  MAC       HP-DLPI DLPI
Path     Address         In# State NamePPA        ID  Type      Support Mjr#
10/12/6  0x0060B032AA2F 0   UP    lan0 snap0     1   ETHER     Yes     119
```

Appendix 15: Contents of /etc/lvmrc

```
# "@(#)/etc/lvmrc       $Revision: 72.2 $$Date: 94/05/20 17:46:54 $"
#
# This file is sourced by /sbin/lvmrc. This file contains the flags
# AUTO_VG_ACTIVATE and RESYNC which are required by the script in /sbin/lvmrc.
# These flags must be set to valid values (see below).
#
#
# The activation of Volume Groups may be customized by setting the
# AUTO_VG_ACTIVATE flag to 0 and customizing the function
# custom_vg_activation()
#

#
#       To disable automatic volume group activation,
#       set AUTO_VG_ACTIVATE to 0.
#

AUTO_VG_ACTIVATE=0

#
#       The variable RESYNC controls the order in which
#       Volume Groups are resyncronized. Allowed values
#       are:
#               "PARALLEL"      - resync all VGs at once.
#               "SERIAL"        - resync VGs one at a time.
#
#       SERIAL will take longer but will have less of an
#       impact on overall I/O performance.
#

RESYNC="SERIAL"


#
#       Add customized volume group activation here.
#       A function is available that will synchronize all
#       volume groups in a list in parallel. It is
#       called parallel_vg_sync.
#
#       This routine is only executed if AUTO_VG_ACTIVATE
#       equals 0.
#

custom_vg_activation()
{
        # e.g. /sbin/vgchange -a y -s
        #       parallel_vg_sync "/dev/vg00 /dev/vg01"
        #       parallel_vg_sync "/dev/vg02 /dev/vg03"

        return 0
}

#
# The following functions should require no additional customization:
#

parallel_vg_sync()
{
        for VG in $*
        do
                {
                if /sbin/vgsync $VG > /dev/null
                then
                        echo "Resynchronized volume group $VG"
                fi
                } &
        done
}
```

Appendix 16: Output of </etc/mount> on stxhpcl1

```
/ on /dev/vg00/lvol3 log on Mon Oct  9 15:57:01 2000
/stand on /dev/vg00/lvol1 defaults on Mon Oct  9 15:57:04 2000
/var on /dev/vg00/lvol8 delaylog,nodatainlog on Mon Oct  9 15:57:18 2000
/usr on /dev/vg00/lvol7 delaylog,nodatainlog on Mon Oct  9 15:57:18 2000
/tmp on /dev/vg00/lvol4 delaylog,nodatainlog on Mon Oct  9 15:57:18 2000
/opt on /dev/vg00/lvol6 delaylog,nodatainlog on Mon Oct  9 15:57:19 2000
/home on /dev/vg00/lvol5 delaylog,nodatainlog on Mon Oct  9 15:57:19 2000
/u01 on /dev/vg01/lv01 delaylog,nodatainlog on Tue Oct 10 09:58:45 2000
/u03 on /dev/vgcl1/lv01 log,nodatainlog on Wed Oct 11 14:40:29 2000
```

Appendix 17: Output of </etc/mount> on stxhpcl2

```
/ on /dev/vg00/lvol3 log on Mon Oct  9 15:52:35 2000
/stand on /dev/vg00/lvol1 defaults on Mon Oct  9 15:52:37 2000
/var on /dev/vg00/lvol8 delaylog,nodatainlog on Mon Oct  9 15:52:51 2000
/usr on /dev/vg00/lvol7 delaylog,nodatainlog on Mon Oct  9 15:52:52 2000
/tmp on /dev/vg00/lvol4 delaylog,nodatainlog on Mon Oct  9 15:52:52 2000
/opt on /dev/vg00/lvol6 delaylog,nodatainlog on Mon Oct  9 15:52:52 2000
/home on /dev/vg00/lvol5 delaylog,nodatainlog on Mon Oct  9 15:52:52 2000
/u01 on /dev/vg01/lv01 delaylog,nodatainlog on Tue Oct 10 10:24:35 2000
/u02 on /dev/vgcl2/lv01 log,nodatainlog on Wed Oct 11 13:32:12 2000
```

Appendix 18: Contents of /etc/rc.config.d/netconf on stxhpcl1

```
# netconf:  configuration values for core networking subsystems
#
# @(#) $Revision: 1.6.119.6 $ $Date: 97/09/10 15:56:01 $
#
# HOSTNAME:            Name of your system for uname -S and hostname
#
# OPERATING_SYSTEM:    Name of operating system returned by uname -s
#                      ---- DO NOT CHANGE THIS VALUE ----
#
# LOOPBACK_ADDRESS:    Loopback address
#                      ---- DO NOT CHANGE THIS VALUE ----
#
# IMPORTANT:  for 9.x-to-10.0 transition, do not put blank lines between
# the next set of statements

HOSTNAME="stxhpcl1"
OPERATING_SYSTEM=HP-UX
LOOPBACK_ADDRESS=127.0.0.1

# Internet configuration parameters.  See ifconfig(1m), autopush(1m)
#
# INTERFACE_NAME:      Network interface name (see lanscan(1m))
#
# IP_ADDRESS:          Hostname (in /etc/hosts) or IP address in decimal-dot
#                      notation (e.g., 192.1.2.3)
#
# SUBNET_MASK:         Subnetwork mask in decimal-dot notation, if different
#                      from default
#
# BROADCAST_ADDRESS:   Broadcast address in decimal-dot notation, if
#                      different from default
#
# INTERFACE_STATE:     Desired interface state at boot time.
#                      either up or down, default is up.
#
# DHCP_ENABLE          Determines whether or not DHCP client functionality
#                      will be enabled on the network interface (see
#                      auto_parms(1M), dhcpclient(1M)). DHCP clients get
#                      their IP address assignments from DHCP servers.
#                      1 enables DHCP client functionality; 0 disables it.
#
# For each additional network interfaces, add a set of variable assignments
# like the ones below, changing the index to "[1]", "[2]" et cetera.
#
# IMPORTANT:  for 9.x-to-10.0 transition, do not put blank lines between
# the next set of statements

INTERFACE_NAME[0]="lan0"
IP_ADDRESS[0]="10.225.69.20"
SUBNET_MASK[0]="255.255.255.0"
BROADCAST_ADDRESS[0]=""
INTERFACE_STATE[0]=""
DHCP_ENABLE[0]=0

# Internet routing configuration.  See route(1m), routing(7)
#
# ROUTE_DESTINATION:   Destination hostname (in /etc/hosts) or host or network
#                      IP address in decimal-dot notation, preceded by the word
#                      "host" or "net"; or simply the word "default".
#
# ROUTE_MASK:          Subnetwork mask in decimal-dot notation, or C language
#                      hexadecimal notation.  This is an optional field.
#                      A IP address, subnet mask pair uniquely identifies
#                      a subnet to be reached. If a subnet mask is not given,
#                      then the system will assign the longest subnet mask
#                      of the configured network interfaces to this route.
#                      If there is no matching subnet mask, then the system
```

```
#                       will assign the default network mask as the route's
#                       subnet mask.
#
# ROUTE_GATEWAY:        Gateway hostname (in /etc/hosts) or IP address in
#                       decimal-dot notation.  If local interface, must use the
#                       same form as used for IP_ADDRESS above (hostname or
#                       decimal-dot notation). If loopback interface, i.e.,
#                      127.0.0.1, the ROUTE_COUNT must be set to zero.
#
# ROUTE_COUNT:          An integer that indicates whether the gateway is a
#                       remote interface (one) or the local interface (zero)
#                      or loopback interface (e.g., 127.*).
#
# ROUTE_ARGS:           Route command arguments and options.  This variable
#                       may contain a combination of the following arguments:
#                       "-f", "-n" and "-p pmtu".
#
# For each additional route, add a set of variable assignments like the ones
# below, changing the index to "[1]", "[2]" et cetera.
#
# IMPORTANT:  for 9.x-to-10.0 transition, do not put blank lines between
# the next set of statements

ROUTE_DESTINATION[0]="default"
ROUTE_MASK[0]=""
ROUTE_GATEWAY[0]="10.225.69.20"
ROUTE_COUNT[0]="0"
ROUTE_ARGS[0]=""

# Dynamic routing daemon configuration.  See gated(1m)
#
# GATED:        Set to 1 to start gated daemon.
# GATED_ARGS:   Arguments to the gated daemon.

GATED=0
GATED_ARGS=""

#
# Router Discover Protocol daemon configuration.  See rdpd(1m)
#
# RDPD:         Set to 1 to start rdpd daemon
#

RDPD=0

#
# Reverse ARP daemon configuration.  See rarpd(1m)
#
# RARP:         Set to 1 to start rarpd daemon
#

RARP=0
```

Appendix 19: Contents of /etc/rc.config.d/netconf on stxhpcl2

```
# netconf:  configuration values for core networking subsystems
#
# @(#) $Revision: 1.6.119.6 $ $Date: 97/09/10 15:56:01 $
#
# HOSTNAME:            Name of your system for uname -S and hostname
#
# OPERATING_SYSTEM:    Name of operating system returned by uname -s
#                      ---- DO NOT CHANGE THIS VALUE ----
#
# LOOPBACK_ADDRESS:    Loopback address
#                      ---- DO NOT CHANGE THIS VALUE ----
#
# IMPORTANT:  for 9.x-to-10.0 transition, do not put blank lines between
# the next set of statements

HOSTNAME="stxhpcl2"
OPERATING_SYSTEM=HP-UX
LOOPBACK_ADDRESS=127.0.0.1

# Internet configuration parameters.  See ifconfig(1m), autopush(1m)
#
# INTERFACE_NAME:      Network interface name (see lanscan(1m))
#
# IP_ADDRESS:          Hostname (in /etc/hosts) or IP address in decimal-dot
#                      notation (e.g., 192.1.2.3)
#
# SUBNET_MASK:         Subnetwork mask in decimal-dot notation, if different
#                      from default
#
# BROADCAST_ADDRESS:   Broadcast address in decimal-dot notation, if
#                      different from default
#
# INTERFACE_STATE:     Desired interface state at boot time.
#                      either up or down, default is up.
#
# DHCP_ENABLE          Determines whether or not DHCP client functionality
#                      will be enabled on the network interface (see
#                      auto_parms(1M), dhcpclient(1M)). DHCP clients get
#                      their IP address assignments from DHCP servers.
#                      1 enables DHCP client functionality; 0 disables it.
#
# For each additional network interfaces, add a set of variable assignments
# like the ones below, changing the index to "[1]", "[2]" et cetera.
#
# IMPORTANT:  for 9.x-to-10.0 transition, do not put blank lines between
# the next set of statements

INTERFACE_NAME[0]=lan0
IP_ADDRESS[0]=10.225.69.21
SUBNET_MASK[0]=255.255.255.0
BROADCAST_ADDRESS[0]=""
INTERFACE_STATE[0]=""
DHCP_ENABLE[0]=0

# Internet routing configuration.  See route(1m), routing(7)
#
# ROUTE_DESTINATION:   Destination hostname (in /etc/hosts) or host or network
#                      IP address in decimal-dot notation, preceded by the word
#                      "host" or "net"; or simply the word "default".
#
# ROUTE_MASK:          Subnetwork mask in decimal-dot notation, or C language
#                      hexadecimal notation.  This is an optional field.
#                      A IP address, subnet mask pair uniquely identifies
#                      a subnet to be reached. If a subnet mask is not given,
#                      then the system will assign the longest subnet mask
#                      of the configured network interfaces to this route.
#                      If there is no matching subnet mask, then the system
#                      will assign the default network mask as the route's
```

```
#                       subnet mask.
#
# ROUTE_GATEWAY:        Gateway hostname (in /etc/hosts) or IP address in
#                       decimal-dot notation.  If local interface, must use the
#                       same form as used for IP_ADDRESS above (hostname or
#                       decimal-dot notation). If loopback interface, i.e.,
#                      127.0.0.1, the ROUTE_COUNT must be set to zero.
#
# ROUTE_COUNT:          An integer that indicates whether the gateway is a
#                       remote interface (one) or the local interface (zero)
#                      or loopback interface (e.g., 127.*).
#
# ROUTE_ARGS:           Route command arguments and options.  This variable
#                       may contain a combination of the following arguments:
#                       "-f", "-n" and "-p pmtu".
#
# For each additional route, add a set of variable assignments like the ones
# below, changing the index to "[1]", "[2]" et cetera.
#
# IMPORTANT:  for 9.x-to-10.0 transition, do not put blank lines between
# the next set of statements

# ROUTE_DESTINATION[0]=default
# ROUTE_MASK[0]=""
# ROUTE_GATEWAY[0]=""
# ROUTE_COUNT[0]=""
# ROUTE_ARGS[0]=""

# Dynamic routing daemon configuration.  See gated(1m)
#
# GATED:        Set to 1 to start gated daemon.
# GATED_ARGS:   Arguments to the gated daemon.

GATED=0
GATED_ARGS=""

#
# Router Discover Protocol daemon configuration.  See rdpd(1m)
#
# RDPD:         Set to 1 to start rdpd daemon
#

RDPD=0

#
# Reverse ARP daemon configuration.  See rarpd(1m)
#
# RARP:         Set to 1 to start rarpd daemon
#

RARP=0

ROUTE_GATEWAY[0]=10.225.69.21
ROUTE_COUNT[0]=0
ROUTE_DESTINATION[0]=default
```

Appendix 20: Output of <netstat -nr> on stxhpcl1

```
Routing tables
Dest/Netmask            Gateway            Flags   Refs      Use  Interface   Pmtu
127.0.0.1               127.0.0.1          UH         0    95871  lo0         4136
10.225.69.20            10.225.69.20       UH         0    18413  lan0        4136
10.225.69.22            10.225.69.22       UH         0        0  lan0:1      4136
10.225.69.0             10.225.69.20       U          3        0  lan0        1500
10.225.69.0             10.225.69.22       U          3        0  lan0:1      1500
127.0.0.0               127.0.0.1          U          0        0  lo0         4136
default                 10.225.69.20       U          0        0  lan0        1500
```

Appendix 21: Output of <netstat -nr> on stxhpcl2

```
Routing tables
Dest/Netmask            Gateway            Flags   Refs      Use  Interface   Pmtu
127.0.0.1               127.0.0.1          UH         0    73359  lo0         4136
10.225.69.21            10.225.69.21       UH         0    11695  lan0        4136
10.225.69.23            10.225.69.23       UH         0        0  lan0:1      4136
10.225.69.0             10.225.69.21       U          3        0  lan0        1500
10.225.69.0             10.225.69.23       U          3        0  lan0:1      1500
127.0.0.0               127.0.0.1          U          0        0  lo0         4136
default                 10.225.69.21       U          0        0  lan0        1500
```

Appendix 22: Contents of /etc/passwd on stxhpcl1

```
root:/asrkIyd.U98c:0:3::/:/sbin/sh
daemon:*:1:5::/:/sbin/sh
bin:*:2:2::/usr/bin:/sbin/sh
sys:*:3:3::/:
adm:*:4:4::/var/adm:/sbin/sh
uucp:*:5:3::/var/spool/uucppublic:/usr/lbin/uucp/uucico
lp:*:9:7::/var/spool/lp:/sbin/sh
nuucp:*:11:11::/var/spool/uucppublic:/usr/lbin/uucp/uucico
hpdb:*:27:1:ALLBASE:/:/sbin/sh
nobody:*:-2:-2::/:
www:*:30:1::/:
oracle:fdOR4rxfx4GVs:101:101:,,,:/home/oracle:/usr/bin/ksh
oneworld:M9r.tGLRzhIWo:102:102:,,,:/home/oneworld:/usr/bin/ksh
owuser1:0q/e8hg5y5geo:103:102:,,,:/home/owuser1:/usr/bin/ksh
```

Appendix 23: Contents of /etc/passwd on stxhpcl2

```
root:8fdfhLf20HJWk:0:3::/:/sbin/sh
daemon:*:1:5::/:/sbin/sh
bin:*:2:2::/usr/bin:/sbin/sh
sys:*:3:3::/:
adm:*:4:4::/var/adm:/sbin/sh
uucp:*:5:3::/var/spool/uucppublic:/usr/lbin/uucp/uucico
lp:*:9:7::/var/spool/lp:/sbin/sh
nuucp:*:11:11::/var/spool/uucppublic:/usr/lbin/uucp/uucico
hpdb:*:27:1:ALLBASE:/:/sbin/sh
nobody:*:-2:-2::/:
www:*:30:1::/:
oracle:R6bu57ElPaWbk:101:101:,,,:/home/oracle:/usr/bin/ksh
oneworld:mkE94U1gpB6.k:102:102:,,,:/home/oneworld:/usr/bin/ksh
owuser1:HFi9CPzs0f0yw:103:102:,,,:/home/owuser1:/usr/bin/ksh
```

Appendix 24: Contents of /etc/services

```
# @(#)services $Revision: 1.32.214.7 $ $Date: 97/09/10 14:50:42 $
#
# This file associates official service names and aliases with
# the port number and protocol the services use.
#
# Some of the services represented below are not supported on HP-UX.
# They are provided solely as a reference.
#
# The form for each entry is:
# <official service name>  <port number/protocol name>  <aliases>
#
# See the services(4) manual page for more information.
# Note: The entries cannot be preceded by a blank space.
#
tcpmux          1/tcp                   # TCP port multiplexer (RFC 1078)
echo            7/tcp                   # Echo
echo            7/udp                   #
discard         9/tcp   sink null       # Discard
discard         9/udp   sink null       #
systat         11/tcp   users           # Active Users
daytime        13/tcp                   # Daytime
daytime        13/udp                   #
qotd           17/tcp   quote           # Quote of the Day
chargen        19/tcp   ttytst source   # Character Generator
chargen        19/udp   ttytst source   #
ftp-data       20/tcp                   # File Transfer Protocol (Data)
ftp            21/tcp                   # File Transfer Protocol (Control)
telnet         23/tcp                   # Virtual Terminal Protocol
smtp           25/tcp                   # Simple Mail Transfer Protocol
time           37/tcp   timeserver      # Time
time           37/udp   timeserver      #
rlp            39/udp   resource        # Resource Location Protocol
whois          43/tcp   nicname         # Who Is
domain         53/tcp   nameserver      # Domain Name Service
domain         53/udp   nameserver      #
bootps         67/udp                   # Bootstrap Protocol Server
bootpc         68/udp                   # Bootstrap Protocol Client
tftp           69/udp                   # Trivial File Transfer Protocol
rje            77/tcp   netrjs          # private RJE Service
finger         79/tcp                   # Finger
http           80/tcp   www             # World Wide Web HTTP
http           80/udp   www             # World Wide Web HTTP
link           87/tcp   ttylink         # private terminal link
supdup         95/tcp                   #
hostnames     101/tcp   hostname        # NIC Host Name Server
tsap          102/tcp iso_tsap iso-tsap # ISO TSAP (part of ISODE)
pop           109/tcp postoffice pop2 # Post Office Protocol - Version 2
pop3          110/tcp  pop-3           # Post Office Protocol - Version 3
portmap       111/tcp  sunrpc          # SUN Remote Procedure Call
portmap       111/udp  sunrpc          #
ident         113/tcp  authentication  # RFC1413
sftp          115/tcp                  # Simple File Transfer Protocol
uucp-path     117/tcp                  # UUCP Path Service
nntp          119/tcp  readnews untp   # Network News Transfer Protocol
ntp           123/udp                  # Network Time Protocol
netbios_ns    137/tcp                  # NetBIOS Name Service
netbios_ns    137/udp                  #
netbios_dgm   138/tcp                  # NetBIOS Datagram Service
netbios_dgm   138/udp                  #
netbios_ssn   139/tcp                  # NetBIOS Session Service
netbios_ssn   139/udp                  #
bftp          152/tcp                  # Background File Transfer Protocol
snmp          161/udp  snmpd           # Simple Network Management Protocol Agent
snmp-trap     162/udp  trapd           # Simple Network Management Protocol Traps
bgp           179/tcp                  # Border Gateway Protocol
# PV performance tool services entries
pvserver      382/tcp    # PV server
```

```
pvalarm      383/tcp    # PV alarm management
#
# UNIX services
#
biff          512/udp  comsat          # mail notification
exec          512/tcp                 # remote execution, passwd required
login         513/tcp                 # remote login
who           513/udp  whod            # remote who and uptime
shell         514/tcp  cmd             # remote command, no passwd used
syslog        514/udp                 # remote system logging
printer       515/tcp  spooler         # remote print spooling
talk          517/udp                 # conversation
ntalk         518/udp                 # new talk, conversation
route         520/udp  router routed   # routing information protocol
efs           520/tcp                 # Extended file name server
timed         525/udp  timeserver      # remote clock synchronization
tempo         526/tcp  newdate         #
courier       530/tcp  rpc             #
conference    531/tcp  chat            #
netnews       532/tcp  readnews        #
netwall       533/udp                 # Emergency broadcasting
uucp          540/tcp  uucpd           # uucp daemon
remotefs      556/tcp  rfs_server rfs  # Brunhoff remote filesystem
ingreslock   1524/tcp                 #
#
# Other HP-UX services
#
lansrm        570/udp                 # SRM/UX Server
DAServer      987/tcp                 # SQL distributed access
instl_boots  1067/udp                 # installation bootstrap protocol server
instl_bootc  1068/udp                 # installation bootstrap protocol client
nfsd-keepalive 1110/udp               # Client status info
nfsd-status    1110/tcp               # Cluster status info
msql         1111/tcp                 # Mini SQL database server
rlb          1260/tcp                 # remote loopback diagnostic
clvm-cfg     1476/tcp                 # HA LVM configuration
diagmond     1508/tcp                 # Diagnostic System Manager
nft          1536/tcp                 # NS network file transfer
sna-cs       1553/tcp                 # SNAplus client/server
sna-cs       1553/udp                 # SNAplus client/server
ncpm-pm      1591/udp                 # NCPM Policy Manager
ncpm-hip     1683/udp                 # NCPM Host Information Provider
cvmon        1686/udp                 # Clusterview cvmon-cvmap communication
registrar    1712/tcp                 # resource monitoring service
registrar    1712/udp                 # resource monitoring service
ncpm-ft      1744/udp                 # NCPM File Transfer
psmond       1788/tcp                 # Predictive Monitor
psmond       1788/udp                 # Hardware Predictive Monitor
pmlockd      1889/tcp                 # SynerVision locking daemon
pmlockd      1889/udp                 #
nfsd         2049/udp                 # NFS remote file system
netdist      2106/tcp                 # update(1m) network distribution service
rfa          4672/tcp                 # NS remote file access
veesm        4789/tcp                 # HP VEE service manager
hacl-hb      5300/tcp                 # High Availability (HA) Cluster heartbeat
hacl-gs      5301/tcp                 # HA Cluster General Services
hacl-cfg     5302/tcp                 # HA Cluster TCP configuration
hacl-cfg     5302/udp                 # HA Cluster UDP configuration
hacl-probe   5303/tcp                 # HA Cluster TCP probe
hacl-probe   5303/udp                 # HA Cluster UDP probe
hacl-local   5304/tcp                 # HA Cluster Commands
hacl-test    5305/tcp                 # HA Cluster Test
hacl-dlm     5408/tcp                 # HA Cluster distributed lock manager
lanmgrx.osB  5696/tcp                 # LAN Manager/X for B.00.00 OfficeShare
r4-sna-cs    5707/tcp                 # SNA client/server (up to Release 4.1)
SNAplus      5708/udp                 # SNA logical network A (up to Release 4.1)
r4-sna-ft    5709/tcp                 # SNA file transfer (up to Release 4.1)
hcserver     5710/tcp                 # HP Cooperative Services
grmd         5999/tcp                 # graphics resource manager
spc          6111/tcp                 # sub-process control
desmevt      6868/tcp                 # DE/ Services Monitor, Event Service
```

```
pdclientd    6874/tcp                # Palladium print client daemon
pdeventd     6875/tcp                # Palladium print event daemon
iasqlsvr     7489/tcp                # Information Access
recserv      7815/tcp                # SharedX Receiver Service
ftp-ftam     8868/tcp                # FTP->FTAM Gateway
mcsemon      9999/tcp                # MC/System Environment Monitor
console      10000/tcp               # MC/System Environment console multiplexor
actcp        31766/tcp               # ACT Call Processing Server
#
# Kerberos (Project Athena/MIT) services
#
kerberos5     88/udp   kdc                 # Kerberos 5 kdc
klogin       543/tcp                 # Kerberos rlogin -kfall
kshell       544/tcp  krcmd          # Kerberos remote shell -kfall
ekshell      545/tcp  krcmd          # Kerberos encrypted remote shell -kfall
kerberos     750/udp  kdc            # Kerberos (server) udp -kfall
kerberos     750/tcp  kdc            # Kerberos (server) tcp -kfall
kerberos_master 751/tcp kadmin       # Kerberos kadmin
krbupdate    760/tcp  kreg           # Kerberos registration -kfall
kpasswd      761/tcp  kpwd           # Kerberos "passwd" -kfall
eklogin     2105/tcp                 # Kerberos encrypted rlogin -kfall
# The X10_LI server for each display listens on ports 5800 + display number.
# The X10_MI server for each display listens on ports 5900 + display number.
# The X11 server for each display listens on ports 6000 + display number.
# The X11 font server listens on port 7000.
# Do NOT associate other services with these ports.
# Refer to the X documentation for details.

hpoms-ci-lstn   5403/tcp      #SAP spooler support
hpoms-dps-lstn  5404/tcp      #SAP spooler support
samd            3275/tcp        # sam daemon

dtspc   6112/tcp       #subprocess control
```

Appendix 25: Output of <swlist>

```
# Initializing...
# Contacting target "stxhpcl1"...
#
# Target:  stxhpcl1:/
#

#
# Bundle(s):
#

  B3935BA      A.11.09        MC / Service Guard
  B3935DA      A.11.09        MC / Service Guard
  B5736BA      A.03.20        HA Monitors
  B5736DA      A.03.20        HA Monitors
  B7609BA      A.03.20        Event Monitoring Service
  HPUXEng32RT  B.11.00.01     English HP-UX 32-bit Runtime Environment
  UXCoreMedia  B.11.00.01     HP-UX Media Kit (Reference Only. See Description)
  XSWGR1100    B.11.00.47.08  General Release Patches, November 1999 (ACE)
```

Appendix 26: Contents of /stand/system

```
* Drivers and Subsystems

CentIf
CharDrv
DlkmDrv
GSCtoPCI
PCItoPCI
arp
asp
autofsc
beep
btlan3
c720
cb
ccio
cdfs
clone
core
diag0
diag2
dlkm
dlpi
dmem
echo
fc
fc_arp
fcgsc
fcgsc_lan
ffs
hpstreams
inet
ip
kload
klog
lan2
lasi
ldterm
lv
lvm
maclan
mux2
netdiag1
```

```
netqa
nfs_client
nfs_core
nfs_server
nfsm
nms
nuls
pa_generic_psm
pa_psm
pci
pckt
pipedev
pipemod
ps2
ptem
ptm
pts
rawip
sad
sc
sctl
sdisk
sio
stape
stcpmap
strlog
strpty_included
strtelnet_included
tcp
telm
tels
timod
tirdwr
tlclts
tlcots
tlcotsod
tun
udp
ufs
uipc
vxbase
wsio


* Kernel Device info

dump lvol


* Tunable parameters

STRMSGSZ        65535
bufpages        0
dbc_max_pct     20
maxfiles        2048
maxfiles_lim    2048
maxswapchunks   4096
maxuprc         ((NPROC*8)/10)
maxusers        400
maxvgs          80
msgmap          (MSGTQL+2)
msgmax          65535
msgmnb          65535
msgmni          (NPROC)
msgseg          32767
msgssz          128
msgtql          4096
nfile           (15*NPROC+2048)
nflocks         (NPROC)
ninode          (8*NPROC+2048)
nproc           (((10*MAXUSERS)/3)+128)
```

```
nstrpty          60
nstrtel          (MAXUSERS)
nswapdev         25
semmap           (SEMMNI+2)
semmni           (NPROC*2)
semmns           (SEMMNI*2)
semmnu           (NPROC-4)
semume           128
semvmx           32768
shmmax           0X40000000
shmmni           512
shmseg           32
swapmem_on       0
timeslice        1
unlockable_mem   (MAXUSERS*10)
```

Appendix 27: Output of <vgdisplay -v> on node stxhpcl1

```
--- Volume groups ---
VG Name                     /dev/vgcl1
VG Write Access             read/write
VG Status                   available, exclusive
Max LV                      255
Cur LV                      1
Open LV                     1
Max PV                      16
Cur PV                      4
Act PV                      4
Max PE per PV               1024
VGDA                        8
PE Size (Mbytes)            4
Total PE                    4092
Alloc PE                    4000
Free PE                     92
Total PVG                   0
Total Spare PVs             0
Total Spare PVs in use      0

   --- Logical volumes ---
   LV Name                      /dev/vgcl1/lv01
   LV Status                    available/syncd
   LV Size (Mbytes)             16000
   Current LE                   4000
   Allocated PE                 4000
   Used PV                      4


   --- Physical volumes ---
   PV Name                      /dev/dsk/c0t1d0
   PV Status                    available
   Total PE                     1023
   Free PE                      0

   PV Name                      /dev/dsk/c0t9d0
   PV Status                    available
   Total PE                     1023
   Free PE                      0

   PV Name                      /dev/dsk/c0t10d0
   PV Status                    available
   Total PE                     1023
   Free PE                      0

   PV Name                      /dev/dsk/c0t11d0
   PV Status                    available
   Total PE                     1023
   Free PE                      92
```

224472 Paula

Appendix 28: Output of <vgdisplay -v> on node stxhpcl2

```
--- Volume groups ---
VG Name                     /dev/vgcl2
VG Write Access             read/write
VG Status                   available, exclusive
Max LV                      255
Cur LV                      1
Open LV                     1
Max PV                      16
Cur PV                      4
Act PV                      4
Max PE per PV               1024
VGDA                        8
PE Size (Mbytes)            4
Total PE                    4092
Alloc PE                    4000
Free PE                     92
Total PVG                   0
Total Spare PVs             0
Total Spare PVs in use      0

   --- Logical volumes ---
   LV Name                      /dev/vgcl2/lv01
   LV Status                    available/syncd
   LV Size (Mbytes)             16000
   Current LE                   4000
   Allocated PE                 4000
   Used PV                      4


   --- Physical volumes ---
   PV Name                      /dev/dsk/c0t0d0
   PV Status                    available
   Total PE                     1023
   Free PE                      0

   PV Name                      /dev/dsk/c0t12d0
   PV Status                    available
   Total PE                     1023
   Free PE                      0

   PV Name                      /dev/dsk/c0t13d0
   PV Status                    available
   Total PE                     1023
   Free PE                      0

   PV Name                      /dev/dsk/c0t14d0
   PV Status                    available
   Total PE                     1023
   Free PE                      92
```

Appendix 29: OneWorld Xe IEO.ini file on node stxhpcl1

```
; RealTime initialization file INI(IEO)

[IEO]
RegisteredEvents=

[SAMPLE_EVENT]
DS1=DXXXXXXXX
DS2=DYYYYYYYY
DS3=DZZZZZZZZ
```

Appendix 30: OneWorld Xe IEO.ini file on node stxhpcl2

```
; RealTime initialization file INI(IEO)

[IEO]
RegisteredEvents=

[SAMPLE_EVENT]
DS1=DXXXXXXXX
DS2=DYYYYYYYY
DS3=DZZZZZZZZ
```

Appendix 31: OneWorld Xe JDE.ini file on node stxhpcl1

```
; OneWorld initialization file INI(JDE)
; HP9000 specific version - B73.3

[DEBUG]
Output=FILE
Trace=TRUE
ClientLog=1
DebugFile=/u03/oneworld/b733_sp14/log/jdedebug.log
JobFile=/u03/oneworld/b733_sp14/log/jde.log
LogErrors=1
JDETSFile=/u03/oneworld/b733_sp14/log/JDETS.log
RepTrace=0

[TAM]
TAMTraceLevel=0

[MEMORY DEBUG]
Frequency=10000
Full=1

[SVR]
EnvType=1
EnvironmentName=XDEVHPO2
SpecPath=spec
SourcePath=source
ObjectPath=obj
HeaderPath=include
HeaderVPath=includev
BinPath=bin32
LibPath=lib32
LibVPath=libv32
MakePath=make
WorkPath=work
CodeGeneratorPath=cg
ResourcePath=res
HelpPath=helps
NextIDPath=nextid
LibraryListName=XDEVHPO2

[INSTALL]
DefaultSystem=system
ClientPath=client
PackagePath=package
DataPath=data
B733=/u03/oneworld/b733_sp14
Double_Byte=0
LocalCodeSet=WE_ISO88591

[JDEIPC]
ipcTrace=0
maxNumberOfSemaphores=200
startIPCKeyValue=53000

[JDEMAIL]
Rule1=90|OPT|MAILSERVER=mail.jdedwards.com
Rule2=100|DEFAULT|OWMON=OWMON@jdedwards.com
Rule3=110|DEFAULT|JDE_SYSTEM=JDE_System@jdedwards.com
Rule4=120|DEFAULT|WORKFLOW_SYSTEM=Workflow@jdedwards.com
Rule5=130|OPT|MERGELOCAL=1
Rule6=140|OPT|UPDATELOCAL=0

[JDENET]
serviceNameListen=6005
serviceNameConnect=6005
maxNetProcesses=1
maxNetConnections=250
maxKernelProcesses=50
maxKernelRanges=20
```

```
netTrace=0

[JDENET_KERNEL_DEF1]
krnlName=JDENET RESERVED KERNEL
dispatchDLLName=libjdenet.sl
dispatchDLLFunction=JDENET_DispatchMessage
maxNumberOfProcesses=1
numberOfAutoStartProcesses=0

[JDENET_KERNEL_DEF2]
krnlName=UBE KERNEL
dispatchDLLName=libjdeknet.sl
dispatchDLLFunction=JDEK_DispatchUBEMessage
maxNumberOfProcesses=1
numberOfAutoStartProcesses=0

[JDENET_KERNEL_DEF3]
krnlName=REPLICATION KERNEL
dispatchDLLName=libjderepl.sl
dispatchDLLFunction=DispatchRepMessage
maxNumberOfProcesses=1
numberOfAutoStartProcesses=0

[JDENET_KERNEL_DEF4]
krnlName=SECURITY KERNEL
dispatchDLLName=libjdeknet.sl
dispatchDLLFunction=JDEK_DispatchSecurity
maxNumberOfProcesses=1
numberOfAutoStartProcesses=0

[JDENET_KERNEL_DEF5]
krnlName=LOCK MANAGER KERNEL
dispatchDLLName=libtransmon.sl
dispatchDLLFunction=TM_DispatchTransactionManager
maxNumberOfProcesses=1
numberOfAutoStartProcesses=0

[JDENET_KERNEL_DEF6]
krnlName=CALL OBJECT KERNEL
dispatchDLLName=libjdeknet.sl
dispatchDLLFunction=JDEK_DispatchCallObjectMessage
maxNumberOfProcesses=1
numberOfAutoStartProcesses=1

[JDENET_KERNEL_DEF7]
krnlName=JDBNET KERNEL
dispatchDLLName=libjdeknet.sl
dispatchDLLFunction=JDEK_DispatchJDBNETMessage
maxNumberOfProcesses=1
numberOfAutoStartProcesses=0

[JDENET_KERNEL_DEF8]
krnlName=PACKAGE INSTALL KERNEL
dispatchDLLName=libjdeknet.sl
dispatchDLLFunction=JDEK_DispatchPkgInstallMessage
maxNumberOfProcesses=1
numberOfAutoStartProcesses=0

[JDENET_KERNEL_DEF9]
krnlName=SAW KERNEL
dispatchDLLName=libjdesaw.sl
dispatchDLLFunction=JDEK_DispatchSAWMessage
maxNumberOfProcesses=1
numberOfAutoStartProcesses=0

[JDENET_KERNEL_DEF10]
krnlName=SCHEDULER KERNEL
dispatchDLLName=libjdeschr.sl
dispatchDLLFunction=JDEK_DispatchScheduler
maxNumberOfProcesses=1
numberOfAutoStartProcesses=0
```

```
[JDENET_KERNEL_DEF11]
krnlName=PACKAGE BUILD KERNEL
dispatchDLLName=libjdeknet.sl
dispatchDLLFunction=JDEK_DispatchPkgBuildMessage
maxNumberOfProcesses=1
numberOfAutoStartProcesses=0

[JDENET_KERNEL_DEF12]
krnlName=UBE SUBSYSTEM KERNEL
dispatchDLLName=libjdeknet.sl
dispatchDLLFunction=JDEK_DispatchUBESBSMessage
maxNumberOfProcesses=1
numberOfAutoStartProcesses=0

[JDENET_KERNEL_DEF13]
krnlName=WORK FLOW KERNEL
dispatchDLLName=libworkflow.sl
dispatchDLLFunction=JDEK_DispatchWFServerProcess
maxNumberOfProcesses=1
numberOfAutoStartProcesses=0

[JDENET_KERNEL_DEF19]
krnlName=EVN KERNEL
dispatchDLLName=libjdeie.sl
dispatchDLLFunction=JDEK_DispatchITMessage
maxNumberOfProcesses=1
numberOfAutoStartProcesses=0

[JDENET_KERNEL_DEF20]
krnlName=IEO KERNEL
dispatchDLLName=libjdeieo.sl
dispatchDLLFunction=JDEK_DispatchIEOMessage
maxNumberOfProcesses=1
numberOfAutoStartProcesses=0

[NETWORK QUEUE SETTINGS]
UBE Semaphore Key=3600
DefaultPrinterOUTQ=devprn6
JDENETTimeout=60

[BSFN BUILD]
BuildArea=/usr/oneworld/BDEV/b733/packages
OptimizationFlags=+O1
DebugFlags=-g -y -D_DEBUG -DJDEDEBUG
InliningFlags=
DefineFlags=-DKERNEL -DPRODUCTION_VERSION -DNATURAL_ALIGNMENT -D_HPUX_SOURCE
CompilerFlags=-Aa +w1 +z -c
OSReleaseLevel=+DAportable
LinkFlags=-b -z -B symbolic -L/usr/oneworld/BDEV/b733/system/lib -ljdesaw
LinkLibraries=
SimultaneousBuilds=0

[UBE]
UBEDebugLevel=0

[DB SYSTEM SETTINGS]
Version=43
Default User=JDESVR
Default Pwd=
Default Env=XDEVHPO2
Default PathCode=PROD
Base Datasource=ORACLE SVR
Object Owner=JDESVR
Server=corowsn1
Database=owsn1devl
Load Library=libora73.sl
Decimal Shift=Y
Julian Dates=Y
Use Owner=Y
Secured=Y
```

```
Type=O
Library List=
TriggerLibrary=JDBTRIG

[LOCK MANAGER]
Server=hpcluster
AvailableService=TS
RequestedService=NONE

[SERVER ENVIRONMENT MAP]
ADEVASD1=ADEVHPO1
ADEVASD2=ADEVHPO2
ADEVNAO1=ADEVHPO1
ADEVNAO2=ADEVHPO2
ADEVNAS1=ADEVHPO1
ADEVNAS2=ADEVHPO2
ADEVNIS1=ADEVHPO1
ADEVNIS2=ADEVHPO2
ADEVRSO1=ADEVHPO1
ADEVRSO2=ADEVHPO2
ADEVCLA1=ADEVHPO1
ADEVCLA2=ADEVHPO2
PDEVASD1=PDEVHPO1
PDEVASD2=XDEVHPO2
PDEVNAO1=PDEVHPO1
PDEVNAO2=XDEVHPO2
PDEVNAS1=PDEVHPO1
PDEVNAS2=XDEVHPO2
PDEVNIS1=PDEVHPO1
PDEVNIS2=XDEVHPO2
PDEVRSO1=PDEVHPO1
PDEVRSO2=XDEVHPO2
PDEVCLA1=PDEVHPO1
PDEVCLA2=XDEVHPO2
PDEVHPO2=XDEVHPO2


[SECURITY]
User=JDESVR
Password=
DefaultEnvironment=XDEVHPO2
DataSource=ORACLE PVC B733
SecurityServer=hpcluster
ServerPswdFile=FALSE
History=0

[CLUSTER]
PrimaryNode=hpcluster

[JDEITDRV]
DrvCount=3
Drv1=Z:libzdrv.sl
Drv2=RT:librtdrv.sl
Drv3=JDENET:libjdetrdrv.sl

[Interoperability]
RealTimeEvents=*ALL
SaveDoc=0
```

Appendix 32: OneWorld Xe JDE.ini file on node stxhpcl2

```
; OneWorld initialization file INI(JDE)
; HP9000 specific version - B73.3

[DEBUG]
Output=FILE
Trace=TRUE
ClientLog=1
DebugFile=/u02/oneworld/b733_sp14/log/jdedebug.log
JobFile=/u02/oneworld/b733_sp14/log/jde.log
LogErrors=1
JDETSFile=/u02/oneworld/b733_sp14/log/JDETS.log
RepTrace=0

[TAM]
TAMTraceLevel=0

[MEMORY DEBUG]
Frequency=10000
Full=1

[SVR]
EnvType=1
EnvironmentName=XDEVHPO2
SpecPath=spec
SourcePath=source
ObjectPath=obj
HeaderPath=include
HeaderVPath=includev
BinPath=bin32
LibPath=lib32
LibVPath=libv32
MakePath=make
WorkPath=work
CodeGeneratorPath=cg
ResourcePath=res
HelpPath=helps
NextIDPath=nextid
LibraryListName=XDEVHPO2

[INSTALL]
DefaultSystem=system
ClientPath=client
PackagePath=package
DataPath=data
B733=/u02/oneworld/b733_sp14
Double_Byte=0
LocalCodeSet=WE_ISO88591

[JDEIPC]
ipcTrace=0
maxNumberOfSemaphores=200
startIPCKeyValue=33000

[JDEMAIL]
Rule1=90|OPT|MAILSERVER=mail.jdedwards.com
Rule2=100|DEFAULT|OWMON=OWMON@jdedwards.com
Rule3=110|DEFAULT|JDE_SYSTEM=JDE_System@jdedwards.com
Rule4=120|DEFAULT|WORKFLOW_SYSTEM=Workflow@jdedwards.com
Rule5=130|OPT|MERGELOCAL=1
Rule6=140|OPT|UPDATELOCAL=0

[JDENET]
serviceNameListen=6006
serviceNameConnect=6006
maxNetProcesses=1
maxNetConnections=250
maxKernelProcesses=50
maxKernelRanges=20
```

```
netTrace=0

[JDENET_KERNEL_DEF1]
krnlName=JDENET RESERVED KERNEL
dispatchDLLName=libjdenet.sl
dispatchDLLFunction=JDENET_DispatchMessage
maxNumberOfProcesses=1
numberOfAutoStartProcesses=0

[JDENET_KERNEL_DEF2]
krnlName=UBE KERNEL
dispatchDLLName=libjdeknet.sl
dispatchDLLFunction=JDEK_DispatchUBEMessage
maxNumberOfProcesses=1
numberOfAutoStartProcesses=0

[JDENET_KERNEL_DEF3]
krnlName=REPLICATION KERNEL
dispatchDLLName=libjderepl.sl
dispatchDLLFunction=DispatchRepMessage
maxNumberOfProcesses=1
numberOfAutoStartProcesses=0

[JDENET_KERNEL_DEF4]
krnlName=SECURITY KERNEL
dispatchDLLName=libjdeknet.sl
dispatchDLLFunction=JDEK_DispatchSecurity
maxNumberOfProcesses=1
numberOfAutoStartProcesses=0

[JDENET_KERNEL_DEF5]
krnlName=LOCK MANAGER KERNEL
dispatchDLLName=libtransmon.sl
dispatchDLLFunction=TM_DispatchTransactionManager
maxNumberOfProcesses=1
numberOfAutoStartProcesses=0

[JDENET_KERNEL_DEF6]
krnlName=CALL OBJECT KERNEL
dispatchDLLName=libjdeknet.sl
dispatchDLLFunction=JDEK_DispatchCallObjectMessage
maxNumberOfProcesses=1
numberOfAutoStartProcesses=1

[JDENET_KERNEL_DEF7]
krnlName=JDBNET KERNEL
dispatchDLLName=libjdeknet.sl
dispatchDLLFunction=JDEK_DispatchJDBNETMessage
maxNumberOfProcesses=1
numberOfAutoStartProcesses=0

[JDENET_KERNEL_DEF8]
krnlName=PACKAGE INSTALL KERNEL
dispatchDLLName=libjdeknet.sl
dispatchDLLFunction=JDEK_DispatchPkgInstallMessage
maxNumberOfProcesses=1
numberOfAutoStartProcesses=0

[JDENET_KERNEL_DEF9]
krnlName=SAW KERNEL
dispatchDLLName=libjdesaw.sl
dispatchDLLFunction=JDEK_DispatchSAWMessage
maxNumberOfProcesses=1
numberOfAutoStartProcesses=0

[JDENET_KERNEL_DEF10]
krnlName=SCHEDULER KERNEL
dispatchDLLName=libjdeschr.sl
dispatchDLLFunction=JDEK_DispatchScheduler
maxNumberOfProcesses=1
numberOfAutoStartProcesses=0
```

```
[JDENET_KERNEL_DEF11]
krnlName=PACKAGE BUILD KERNEL
dispatchDLLName=libjdeknet.sl
dispatchDLLFunction=JDEK_DispatchPkgBuildMessage
maxNumberOfProcesses=1
numberOfAutoStartProcesses=0

[JDENET_KERNEL_DEF12]
krnlName=UBE SUBSYSTEM KERNEL
dispatchDLLName=libjdeknet.sl
dispatchDLLFunction=JDEK_DispatchUBESBSMessage
maxNumberOfProcesses=1
numberOfAutoStartProcesses=0

[JDENET_KERNEL_DEF13]
krnlName=WORK FLOW KERNEL
dispatchDLLName=libworkflow.sl
dispatchDLLFunction=JDEK_DispatchWFServerProcess
maxNumberOfProcesses=1
numberOfAutoStartProcesses=0

[JDENET_KERNEL_DEF19]
krnlName=EVN KERNEL
dispatchDLLName=libjdeie.sl
dispatchDLLFunction=JDEK_DispatchITMessage
maxNumberOfProcesses=1
numberOfAutoStartProcesses=0

[JDENET_KERNEL_DEF20]
krnlName=IEO KERNEL
dispatchDLLName=libjdeieo.sl
dispatchDLLFunction=JDEK_DispatchIEOMessage
maxNumberOfProcesses=1
numberOfAutoStartProcesses=0

[NETWORK QUEUE SETTINGS]
UBE Semaphore Key=3600
DefaultPrinterOUTQ=devprn6
JDENETTimeout=60

[BSFN BUILD]
BuildArea=/usr/oneworld/BDEV/b733/packages
OptimizationFlags=+O1
DebugFlags=-g -y -D_DEBUG -DJDEDEBUG
InliningFlags=
DefineFlags=-DKERNEL -DPRODUCTION_VERSION -DNATURAL_ALIGNMENT -D_HPUX_SOURCE
CompilerFlags=-Aa +w1 +z -c
OSReleaseLevel=+DAportable
LinkFlags=-b -z -B symbolic -L/usr/oneworld/BDEV/b733/system/lib -ljdesaw
LinkLibraries=
SimultaneousBuilds=0

[UBE]
UBEDebugLevel=0

[DB SYSTEM SETTINGS]
Version=43
Default User=JDESVR
Default Pwd=
Default Env=XDEVHPO2
Default PathCode=PROD
Base Datasource=ORACLE SVR
Object Owner=JDESVR
Server=corowsn1
Database=owsn1devl
Load Library=libora73.sl
Decimal Shift=Y
Julian Dates=Y
Use Owner=Y
Secured=Y
```


```
Type=O
Library List=
TriggerLibrary=JDBTRIG

[LOCK MANAGER]
Server=hpcluster2
AvailableService=TS
RequestedService=NONE

[SERVER ENVIRONMENT MAP]
ADEVASD1=ADEVHPO1
ADEVASD2=ADEVHPO2
ADEVNAO1=ADEVHPO1
ADEVNAO2=ADEVHPO2
ADEVNAS1=ADEVHPO1
ADEVNAS2=ADEVHPO2
ADEVNIS1=ADEVHPO1
ADEVNIS2=ADEVHPO2
ADEVRSO1=ADEVHPO1
ADEVRSO2=ADEVHPO2
ADEVCLA1=ADEVHPO1
ADEVCLA2=ADEVHPO2
PDEVASD1=PDEVHPO1
PDEVASD2=XDEVHPO2
PDEVNAO1=PDEVHPO1
PDEVNAO2=XDEVHPO2
PDEVNAS1=PDEVHPO1
PDEVNAS2=XDEVHPO2
PDEVNIS1=PDEVHPO1
PDEVNIS2=XDEVHPO2
PDEVRSO1=PDEVHPO1
PDEVRSO2=XDEVHPO2
PDEVCLA1=PDEVHPO1
PDEVCLA2=XDEVHPO2
PDEVHPO2=XDEVHPO2


[SECURITY]
User=JDESVR
Password=JDESVR
DefaultEnvironment=XDEVHPO2
DataSource=ORACLE PVC B733
SecurityServer=hpcluster2
ServerPswdFile=TRUE
History=0

[CLUSTER]
PrimaryNode=hpcluster2

[JDEITDRV]
DrvCount=3
Drv1=Z:libzdrv.sl
Drv2=RT:librtdrv.sl
Drv3=JDENET:libjdetrdrv.sl

[Interoperability]
RealTimeEvents=*ALL
SaveDoc=0
```

Appendix 33: HP's Partner Technology Access Center High Availability Implementation and Certification Services Data Sheet

Hewlett-Packard Company has a wide range of powerful high availability tools and services to assist ISVs in the certification of their applications in a highly available, mission-critical Hewlett-Packard environment.

HP's High Availability software tool suite, including MC/ServiceGuard, is a specialized facility for protecting mission-critical applications from hardware and software failures. With MC/ServiceGuard, multiple nodes (systems) are organized into an enterprise cluster that is capable of delivering highly available application services to LAN attached clients.

For ease of management and outstanding flexibility, MC/ServiceGuard allows all of the resources needed by an application to be organized into entities called "application packages". Application packages consist of any resource needed to support a specific application service, such as disks, network resources, and application or system processes. Packages are the entities that are managed and moved within the enterprise cluster.

When an ISV delivers an application that will be run in a mission critical environment, it is important to certify that the application has been configured and tested in an MC/ServiceGuard environment.

To aid ISVs in certifying their applications in a highly available environment, the HP Partner Technology Access Center (PTAC) provides hardware and consulting services. The following are the types of services provided:

- Analysis of Application Environment:
  - system resources used by the application
  - application design and number of packages
  - use of raw, HFS or JFS volumes
  - application recovery methods
  - data loss specifications
  - checkpointing or buffer flushing frequency
  - shared versus replicated file systems for code and/or data
  - use of memory-based data
  - capacity requirements
  - issues affecting failover time

- Cluster configuration of SCC hardware to match your application needs
- Define application packages and resources required
- Create application package control scripts:
  - application startup & shutdown
  - application monitoring
  - application error handling
  - application restart options
  - application IP addresses
  - service names
  - volume group handling
  - data recovery procedures

- Create, verify and execute a test plan which will exercise defined failure scenarios
- Demonstrate the functionality of the highly available cluster

The HP PTAC maintains the following hardware cluster, available for High Availability application certification:

- (2) L2000 2-way SMP processors
  - 4GB RAM per machine
  - 4 LAN interfaces per machine

– 360GB usable disk space

Additionally, the PTAC offers a High Availability Implementation and Verification Service for those ISVs who wish to verify their Windows NT applications with Microsoft Cluster Server.

Contact the Partner Technology Access Center for more information about these and additional services.

HP Partner Technology Access Center
W 120 Century Road
Paramus, NJ 07653
USA
Tel: (1) 516-753-3406

Appendix 34: HP's Partner Technology Access Center High Availability Implementation and Certification Services Process and Methodology

To aid Independent Software Vendors (ISVs) in certifying their applications in a highly available environment, the Hewlett-Packard (HP) Partner Technology Access Center (PTAC) provides hardware, HA training, and consulting services. The following are the types of services provided:

- Analysis of Application Environment
- Cluster configuration of PTAC hardware to match application needs
- Define application packages and resources required
- Create application package control scripts
- Create, verify and execute a test plan which will exercise defined failure scenarios
- Demonstrate the functionality of the highly available cluster

To perform this service, and to offer it as a repeatable deliverable, the PTAC has defined a process and methodology. The completion of this process will result in an ISVs application being certified by HP as being able to perform in a highly available environment.

An ISVs customer either:

- View the ISVs application as mission-critical
- Mandates that the application must be run in a highly available state

However, a typical ISV has limited experience with architecting and testing HA solutions. Additionally, hardware for failover testing is often unavailable.

Initial Activities

- Contact PTAC administration at 1/516-753-3406 and request the HA Certification Services Package.
- Read and share the package with your ISV.
- A knowledgeable engineer from the ISV must be present at the PTAC lab during the entire HA certification.
- If the ISV has an assigned HP TC, that TC may optionally be present for the HA certification.
- Call PTAC administration and schedule PTAC HA Lab time.

Homework

The HA Certification Services Package contains:

- MC/ServiceGuard (MC/SG) manual
- "Designing Highly Available Cluster Applications" white paper
- MS/SG product brief
- Example certification write-up
- Example cluster and package configuration scripts.

The goal of this step is that the ISV should understand HP's HA product family and understand how to architect his application for HA certification.

Planning

- What should the cluster look like during normal operations?
- What is the standard configuration of most customers?
- Can application modules be spread across multiple systems? Is this normal?
- Do all pieces of the application failover together to the failover machine?
- Can applications running on different machines failover to a shared failover machine?
- Is there any HA mechanism already built in to the app?
- What are the customers expectations of HP's HA product suite?

Technical Evaluation

- Evaluate the app per HA design rules
- Discuss each rule with the application engineers
- What does the app do today to handle a system panic or reboot?
- Does the app use any system specific calls (e.g. uname, gethostbyname, SPU_ID, etc.)?

The deliverable of this step is a write-up of any issues.

App Setup Without MC/SG

- Setup the system without MC/ServiceGuard
- Install the app on the primary system
- Install all shared data on separate external volume groups
- Use JFS file systems as appropriate
- Test the app on the primary system
- Perform a "standard" ISV-provided test to ensure the app is running correctly
- If possible, connect to the app through a client
- Crash the primary system, reboot it, and test how the app starts
- Document any manual procedures
- Can everything start from rc scripts?
- Write a script which brings up the app and all required services

The goal of this step is to ensure that the app can automatically be started and shutdown.

The deliverable of this step is the tasks or scripts which start the app automatically.

No MC/SG, 2 Systems

Try to failover the app to the failover system by hand:

- Connect the volume group to the second system, vgimport, create mount points, etc.
- Document what has to be created on the failover system for the certification whitepaper
- With the app NOT running on the primary system, try to bring it up on the failover system
- Repeat this process until the app will run on the failover system

The goal of this step is to ensure that the failover can occur manually.

Hands On with MC/SG

Configure the MC/SG Cluster:

- Cluster configuration
- Create package(s)
- Create package script
- Compile package configuration scripts and distribute
- Use these scripts as the "customer_defined" functions in the package control scripts

The deliverable of this step is the cluster and package scripts.

Testing

Testing should be performed with a client connected and under system load. This is to test how well and how quickly the application recovers from a failover when a large amount of "work" is queued.

- Halt the package on the primary system and move it to the failover system.
- Move the package back to the primary system.
- Fail one of the systems (e.g. power off, kill monitored process, LAN disconnect)
- Ensure that the package starts on the failover system
- Repeat failover from the failover system back to the primary

- Be sure to test all combinations of app load during testing
- Repeat the failover process under different application states (i.e. heavy user load, no user load, batch jobs, online transactions)
- Keep timing records of how long it takes to completely failover the app
- The customer of the ISV will want to know the failover timing as part of the certification process

Application Monitoring

- MC/SG can monitor the health of processes which are critical to the correct running of the app
- Or, a custom monitor script can be written to monitor specific ISV processes
- Monitor script can be written now, or be written at each customer site

Support and Write-up

- The ISV will own the MC/SG scripts, but the SCC will keep copies for our records
- Determine whether the ISV will want to come back to test new application releases
- HP supports MC/SG, and the ISV supports the concept of failover with its application

The PTAC HA engineer will work with the ISV to produce the following deliverables. A copy of these will be placed on the HP Advanced Technology Center (ATC) High Availability web page:

- Whitepaper with technical details of the failover, known issues and recommended configurations
- Package control script
- Package configuration file (ASCII)
- Press release on the integration

Example Timetable

To understand the progression of the HA certification process, here is a typical ISV certification scenario:

- Day 1: ISVs HP contact calls PTAC information line
- Day 2: HA Certification Services information package is e-mailed to HP contact
- Day 3: HP contact reviews documentation, and provides to ISV
- Day 4: ISV reviews documentation to understand what must be done prior to coming to the PTAC HA Lab
- Day 5: ISV reports to HP contact when they will be ready to begin certification process
- Day 5: HP contact schedules PTAC HA Lab and engineering time
- Day 6-10: ISV performs necessary homework in preparation for certification process. ISV gathers all non-HP-UX materials that will be needed for the certification. If so desired, ISV prepares a client machine for delivery to the PTAC HA Lab.
- Day 11: ISV travels to PTAC HA Lab in Paramus, NJ
- Day 12: ISV is given a half day of training on HPs HA product suite
- Day 12: ISV and PTAC engineer begin installation of ISV application on PTAC hardware
- Day 13-Day 17: ISV and PTAC engineer follow the HA certification process noted earlier in this document

Notes:

- This is an example scenario. Timing and process progression will be different for each ISV.
- If the ISV wishes to test a client connection to his application, the ISV must supply the client machine. The PTAC lab will provide PC display monitors and PC keyboards.
- The ISV must provide all non-HP-UX material on 4mm DAT tape or CD-ROM. The PTAC HA Lab servers are on a private subnet, and cannot contact machines outside of the PTAC HA Lab.

For More Information...

To receive the PTAC HA Certification Services Package, leave your name and Telnet at 1/516-753-3406, along with the name of your ISV.

Once you have received and examined the PTAC HA Certification Services Package, you will want to schedule the PTAC lab, as well as a PTAC High Availability engineer. To do so, please leave your name, Telnet, ISV name and timeframe desired, on 1/516-753-3406.

Questions about this process and the PTAC HA Certification Service may be directed to:

Hewlett-Packard Company
Walt Saiko
Partner Technology Access Center
W 120 Century Road
Paramus, NJ 07653
USA
Tel: (1) 301-258-5974

COBRA TECNOLOGIA
Integradora de Soluções em TI e Serviços

244456
Paula

ANEXO UNIDADE DE BACKUP ROBOTIZADO
PARTE D/8

COBRA Tecnologia S.A.
Estrada dos Bandeirantes 7966
CEP 22783-110 Rio de Janeiro RJ
Tel. 21 2442-8800
www.cobra.com.br

0834

1/1

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls:
3685
Doc:

13 Integrations with Other Applications

In This Chapter

This chapter gives detailed information on how to integrate the following applications with Data Protector:

For information on integrations with other applications, such as Microsoft SQL, Oracle8, and many more, refer to the *HP OpenView Storage Data Protector Integration Guide*. For a list of supported integrations, see the Data Protector documentation overview in the preface of this manual.

NOTE Some functionality is subject to specific Data Protector licenses. See the *HP OpenView Storage Data Protector Installation and Licensing Guide* for details.

Cluster Integrations with Data Protector

See the *HP OpenView Storage Data Protector Software Release Notes* for details on the supported cluster software on specific operating systems, level of cluster support and for supported configurations.

See the *HP OpenView Storage Data Protector Concepts Guide* for more information about cluster support and cluster concepts.

See the *HP OpenView Storage Data Protector Integration Guide* for details on Data Protector integrated database applications in a cluster.

Cluster Concepts and Terminology

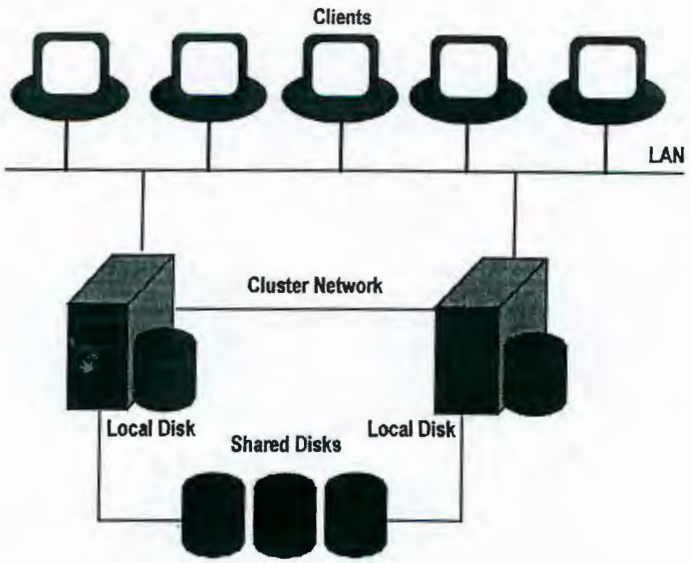
What Is a Cluster?

A **cluster** is a group of two or more independent computers that appear on the network as a single system. This group of computers is managed as a single system and is designed to:

- Ensure that mission-critical applications and resources are as highly available as possible
- Tolerate component failures
- Support either the addition or subtraction of components

Figure 13-1 shows a typical cluster containing the following components:

Figure 13-1 **A Typical Cluster**



- Cluster nodes (two or more)
- Local disks
- Shared disks (shared between nodes)

Cluster Nodes

Cluster nodes are computers that compose a cluster. They are physically connected to one or more shared disks.

Shared Disks

The **shared disks volumes** (MSCS) or **shared volume groups** (MC/SG) or **shared pools** (Novell NetWare Cluster) contain mission-critical application data as well as specific cluster data needed to run the cluster. In MSCS and Novell NetWare clusters, a shared disk/pool is exclusively active on only one cluster node at a time. In MC/SG clusters, the other node can activate the disk in the read only mode.

Cluster Network

Cluster network is a private network that connects all cluster nodes. It transfers the internal cluster data called **heartbeat of the cluster**. The heartbeat is a data packet with a time stamp that is distributed among

all cluster nodes. Each cluster node compares this packet and determines which cluster node is still operational so that appropriate ownership of the **package** (MC/SG, Veritas Cluster) or **group** (MSCS) can be determined.

What is a Package or Group?

A package (MC/SG, Veritas Cluster) or a group (MSCS) is a collection of resources that are needed to run a specific **cluster-aware** application. Each cluster-aware application declares its own critical resources. The following resources must be defined in each group or package:

- Shared disk volumes (MSCS)
- Shared volume groups (MC/SG, Veritas Cluster)
- Network IP names
- Network IP addresses
- Cluster-aware application services

What Is a Virtual Server?

Disk volumes and volume groups represent shared physical disks. A network IP name and a network IP address are resources that define a **virtual server** of a cluster-aware application. Its IP name and address are cached by the cluster software and mapped to the cluster node on which the specific package or group is currently running. Since the group or package can switch from one node to another, the virtual server can reside on different machines in different time frames.

What Is a Failover?

Each package or group has its own preferred node on which it normally runs. Such a node is called a primary node. A package or group can be moved to another cluster node (one of the secondary nodes). The process of transferring a package or group from the primary cluster node to the secondary is called **failover** or switchover. The secondary node accepts the package or group in case of failure of the primary node. A failover can occur for many different reasons:

- Software failures on the primary node
- Hardware failures on the primary node
- The administrator intentionally transfers the ownership because of maintenance on the primary node

NOTE

In MSCS environment, Cluster Service components (for example, Database Manager) maintain a coherent image of the central cluster database, which stores information regarding changes in the status of a node, resource, or group. Cluster database must be stored on the cluster's shared disk volume.

Cluster-Aware Databases and Applications

Data Protector integrates with cluster-aware applications that have already been installed on the cluster as virtual servers, by using the application's virtual server configuration.

To back up the cluster-aware application, use its virtual server name when configuring the backup specification.

Microsoft Cluster Server Integration

As a part of its high-availability functionality and support, Data Protector provides an integration with the Microsoft Cluster Server (MSCS). See the *HP OpenView Storage Data Protector Software Release Notes* for details on the supported cluster software on specific operating systems, level of cluster support and for supported configurations.

NOTE

This section provides specific information for integration of Data Protector and Microsoft Cluster Server.

It is assumed that you are familiar with clustering concepts and concepts related to the Microsoft Cluster Server.

Refer to the following manuals for more information:

- Microsoft Cluster Server online documentation.
- *HP OpenView Storage Data Protector Installation and Licensing Guide* for more information on how to install Data Protector.
- *HP OpenView Storage Data Protector Software Release Notes* for last minute information on the current Data Protector release.

Licensing and Microsoft Cluster Server

When you purchase a license for the Data Protector Cell Manager, note that the license will be bound to the virtual server and will work regardless of which physical node inside a Microsoft Cluster Server runs the Data Protector Cell Manager.

The integration is provided on two levels, Cell Manager or client:

- The Data Protector Cell Manager can be installed on the Microsoft Cluster Server, thus providing higher availability of the Data Protector Cell Manager.
- Data Protector cluster client supports a filesystem backup in a cluster environment and backup of the cluster-aware applications.

Cell Manager on Microsoft Cluster Server

The Data Protector Cell Manager can be installed on the 32-bit Microsoft Cluster Server. This enables an automatic migration of the Data Protector services from one cluster node to another in case of failover.

Installation

See the *HP OpenView Storage Data Protector Installation and Licensing Guide* for more information on how to install Data Protector cluster Cell Manager.

After setup finishes, the Data Protector cluster cell has the following systems automatically added:

- All cluster nodes
- All cluster virtual servers

Clients on Microsoft Cluster Server

Data Protector can back up a full cluster (local and shared disks) and applications running in a cluster environment.

Installation

To back up a cluster-aware application the Data Protector client software must be installed locally on all the cluster nodes. See the *HP OpenView Storage Data Protector Installation and Licensing Guide* for information on how to install a cluster-aware client.

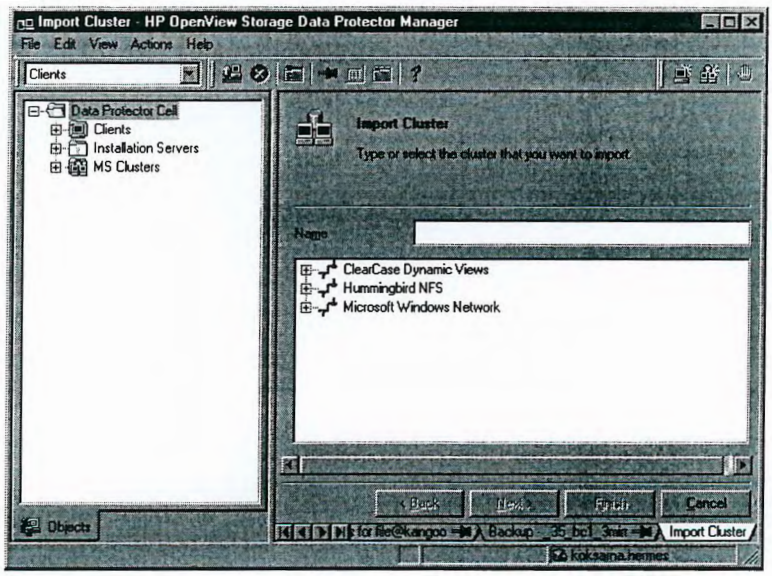
Configuration

After the installation, virtual server hostname of the client must be imported to the Data Protector cell. See the Figure 13-2 on page 619 and the *HP OpenView Storage Data Protector Installation and Licensing Guide* for instructions.

NOTE

If you want an application backup to be cluster-aware, that is, access it through its virtual server, also this application integration module has to be installed on each application preferred owners (nodes). Only this way the Data Protector integration agents can start on cluster nodes where the application currently resides.

Figure 13-2 **Importing Cluster Virtual Server Hostnames to a Cell on Microsoft Cluster Server**



Backing Up Data in a Cluster (MSCS)

When backing up data that reside on cluster node disks, you need to distinguish between:

- Local cluster node disks
- Shared cluster node disks

In the Data Protector GUI, you can see only local disks listed for each cluster node. On the other hand, you can see cluster virtual server items that contain only shared disks for the group in which they are defined. This prevents creation of a backup specification for backing up shared disks. Such backup would fail in case the shared disks are not available on a specific cluster node.

To distinguish between local cluster node disks and shared cluster node disks, Data Protector queries the MSCS database for a list of physical cluster disk resources. All cluster disks presented as proprietary cluster disk resources (e.g. NetRAID 4 disk type) are treated as local cluster node disks.

However, when creating a backup specification, you can see three or more systems that can be backed up:

- Primary node (selected when backing up local disks)
- Secondary node(s) (selected when backing up local disks)
- Virtual server(s) (selected when backing up shared disks)

Backing Up Local Disks

To back up cluster local disks, proceed as follows:

1. Install and configure the Data Protector Disk Agent and cluster component on each cluster node that has the local disks you want to back up.
2. Configure a backup specification for specific cluster node and select which of its local disks you want to back up.

Backing Up Shared Disks

To back up cluster shared disks, proceed as follows:

1. Install (locally) the Data Protector cluster client software on each cluster node. See the *HP OpenView Storage Data Protector Installation and Licensing Guide* for instructions.
2. Import virtual server hostname (Microsoft Cluster Server) to the Data Protector cell. See the *HP OpenView Storage Data Protector Installation and Licensing Guide* for instructions.
3. Configure a backup specification for the virtual server and select the shared disks you want to back up.

Managing Cluster-Aware Backups

In the Data Protector cluster Cell Manager, the backup session is cluster-aware. You can set options that define backup behavior if a failover of Data Protector or other cluster-aware applications occurs.

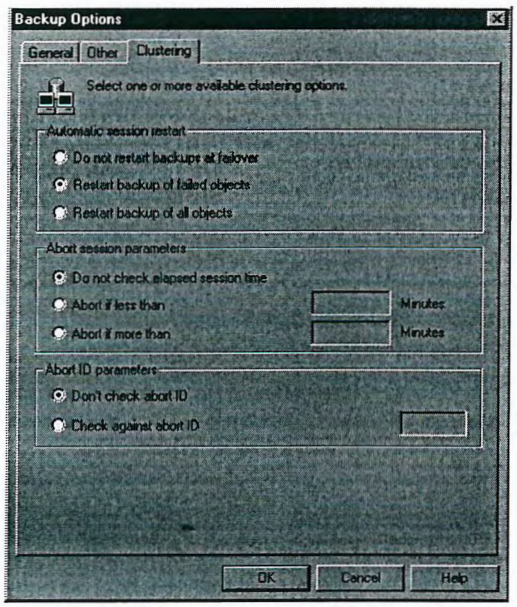
Failover of Data Protector

If a failover of the cluster-aware Data Protector occurs during backup, all running and pending backup sessions fail. In the Data Protector GUI and in the backup specification, you can set one of the options that define automatic backup session restart at failover of Data Protector. See Figure 13-3 on page 622.

Automating Restart of Failed Sessions To modify a backup specification, either filesystem or integration, so that the running backup sessions are automatically restarted at failover of the Cell Manager, perform the following steps:

1. In the `HP OpenView Storage Data Protector Manager`, switch to the `Backup` context, expand the `Backup Specifications` item, and select the backup specification that you would like to modify.
2. In the Results Area, click `Options`.
3. Under the `Backup Specification Options`, click `Advanced`.
4. In the `Backup Options` window, click `Clustering` and select one of the `Automatic session restart` options.

Figure 13-3 Advanced Backup Specification Options-Clustering



Do not Restart Backups At Failover

When the `Do not restart backups at failover` option is selected, sessions that failed are not restarted. This is the default option.

Restart Backup of Failed Objects

The `Restart backup of failed objects` option is only valid for a filesystem backup specification and specifies that completed objects within the filesystem backup specification will not be restarted. Only objects that failed (running or pending at the moment of the failover) will be restarted. This can minimize the backup time in case failover occurs after some backup objects have been completed.

Restart Backups of All Objects

The `Restart backups of all objects` option is valid for both filesystem and integration backup specifications. When this option is selected, the entire session will be restarted after failover, including the objects that have been completed.

Failover of Application Other Than Data Protector

As the Data Protector cluster Cell Manager is a storage application within a cluster environment, it has to be aware of other applications that might be running within the cluster. If they are running on a node other than Data Protector and if some application fails over to the node where Data Protector is running, this will result in a high load on this node. The node that previously managed only backup operations has now to handle critical application requests as well. Data Protector allows you to define what should happen in such a situation so that the critical application data is protected and the load is balanced again. You can:

- Abort all running backup sessions
- Abort specific running backup sessions
- Inhibit the Data Protector cluster Cell Manager for a specific time frame

Aborting All Running Sessions If the backup is less important than the application, Data Protector can automatically abort all running sessions to balance the load after failover of the application.

To define this option use the `omniclus` command. This command is used as part of a script that is run when a failover of the application occurs. You need to create this script in advance and define it as a new resource type in the application group.

To create the script that will abort all running sessions at failover of the application other than Data Protector, perform the following steps:

1. In the *<Data_Protector_home>*`\bin` directory create a batch file with the following command line:

   ```
   omniclus.exe -clus <Data_Protector_virtual_server>
   -session * -abortsess
   ```

NOTE The * wild card represents all sessions. It can be replaced with the name of a specific backup specification in order to abort only this specific backup session.

2. Open the Windows Cluster Administrator and add a new resource to the application group. For `Resource type` select `Generic Application`. For `Possible owners` select the node on which this

script will be run. This is the node where Data Protector is running. In the Generic Application Parameters window, enter the path name of batch file (for example, c:\program_files\omniback\bin\clus.bat) and directory of the omniclus command. This command resides in the *<Data_Protector_home>*\bin directory.

Examples

To abort all running sessions on the server obsv.company.com use the following command line:

```
omniclus.exe -clus obvs.company.com -session * -abortsess
```

To abort only session from a backup specification backup_1 on the server obsv.company.com use the following command line:

```
omniclus.exe -clus obvs.company.com -session backup_1
-abortsess
```

Aborting Running Sessions Based on a Logical ID If a specific running backup session is more important than the application, Data Protector can continue this session. To balance the load after a failover, you can abort all backup sessions except an important one using its abort ID. You define this option by using the Data Protector GUI and scripting.

Proceed as follows:

Data Protector GUI

1. In the Data Protector GUI, modify the backup specification with the following steps:
   a. In the HP OpenView Storage Data Protector Manager, switch to the Backup context, expand the Backup Specifications item, and select the backup specification that you would not like to be aborted at failover of the application.
   b. In the Results Area, click Options.
   c. Under Backup Specification Options, click Advanced.
   d. In the Backup Options window, click Clustering. Select Check against abort ID and enter a backup specification ID that will represent this specification and will be used in the command line.

Command Line

2. In the batch file, modify the omniclus command as follows:

```
omniclus.exe -clus <Data Protector_virtual_server>
-session <backup_specification> -abortsess -abortid
<logical_operator_ID>
```

Example

In the Data Protector GUI you have configured a backup specification with abort ID = 10. Use the following command line to abort all backup sessions except one with abort ID = 10 on the server `obsv.company.com`:

```
omniclus.exe -clus obvs.company.com -session * -abortsess
-abortid != 10
```

Aborting Sessions Based on Elapsed Session Time To balance the load after a failover you can abort backup sessions based on how long they have already been running. If a specific running backup session is just ending, Data Protector can continue the session. If the backup session has just started and if it is not important, Data Protector can abort the session. You define this option by using the Data Protector GUI and scripting.

Proceed as follows:

Data Protector GUI

1. In the Data Protector GUI, modify the backup specification with the following steps:
   a. In the `HP OpenView Storage Data Protector Manager`, switch to the `Backup` context, expand the `Backup Specifications` item, and select the backup specification that you would like to be aborted based on elapsed session time.
   b. In the Results Area, click `Options`.
   c. Under `Backup Specification Options`, click `Advanced`.
   d. In the `Backup Options` window, click `Clustering`. Select `Abort if less than` or `Abort if more than` and enter the minutes that will represent this specification. It will be aborted if the specified condition is fulfilled when a failover occurs.

Command Line

2. In the batch file, modify the `omniclus` command as follows:

```
omniclus.exe -clus <Data Protector_virtual_server>
-session * -abortsess
```

NOTE When the command is run, the elapsed time for each backup specification is checked and the session is aborted if the specified conditions are met. For example, in the Data Protector GUI specify that the backup specification is aborted if it has been running for less than 30 minutes. When the failover occurs and when the `omniclus` command is started, the session is aborted if it has been running for less than 30 minutes, otherwise it continues.

Temporarily Disabling Backup Sessions To balance the load after a failover, you can also disable the Cell Manager for some time. All running session are continuing but you cannot start new backups until the Cell Manager is enabled again. You define this only by using scripting.

Command Line In the batch file, modify the `omniclus` command as follows:

```
omniclus.exe -clus <Data Protector_virtual_server> -inhibit
minutes
```

Examples To disable new backups on the server `obvs.company.com` for 20 minutes, use the following command line:

```
omniclus.exe -clus obvs.company.com -inhibit 20
```

To disable new backups until the Cell Manager is enabled again, use the following command line:

```
omniclus.exe -clus obvs.company.com -inhibit *
```

To enable backups again, run the following command line in CLI:

```
<Data_Protector_home>\bin\omniclus -clus obvs.company.com
-inhibit 0
```

MC/ServiceGuard Integration

As part of its high-availability support, Data Protector provides a full integration of the Data Protector Cell Manager with MC/ServiceGuard on HP-UX systems. For details on supported operating system versions, supported configurations, and level of cluster support, refer to the *HP OpenView Storage Data Protector Software Release Notes*.

NOTE

This section provides specific information for integration of Data Protector and MC/ServiceGuard.

It is assumed that you are familiar with clustering concepts and concepts related to MC/ServiceGuard.

Refer to the following manuals for more information:

- *Managing MC/ServiceGuard* for more information on MC/ServiceGuard.
- *HP OpenView Storage Data Protector Installation and Licensing Guide* for more information on how to install Data Protector.
- *HP OpenView Storage Data Protector Software Release Notes* for last minute information on the current Data Protector release.

Licensing and MC/ServiceGuard

When you purchase a license for the Data Protector Cell Manager, note that the license will be bound to the cluster package and will work regardless of which physical node inside an MC/ServiceGuard cluster runs the Data Protector Cell Manager, so long as the package is running on one of the nodes.

Cell Manager on MC/ServiceGuard

Prerequisites

- In an MC/ServiceGuard cluster environment, a Data Protector Cell Manager should have its own package. Before installing Data Protector Cell Manager on MC/ServiceGuard, you need to get the following information from your network administrator:
  - Package name or virtual hostname

— Package IP or virtual ip-address

In addition, you will also need to create a volume group on a shared disk.

- Ensure that the cluster nodes and the package IP are on the same subnet.
- If you have DNS in your environment, ensure that all the cluster nodes and the package IP are registered with the DNS server.

Installation

Install all hosts in the cluster using the standard procedure for installing the Cell Manager on UNIX as described in the *HP OpenView Storage Data Protector Installation and Licensing Guide*.

IMPORTANT

If you need to add additional software components on cluster nodes using the GUI, make sure that the node to which you add the components is active.

Configuration

Prerequisites for Configuration

Before you start configuring Data Protector with MC/ServiceGuard, check the following:

- The cluster should be installed and running.
- Decide which systems are going to be the Primary Cell Manager and the Secondary Cell Manager(s).
- Systems chosen to be the Primary Cell Manager and the Secondary Cell Manager(s) must have MC/ServiceGuard installed, with recommended patches, and must be configured as members of the same cluster. For instructions on MC/ServiceGuard installation and configuration, refer to the *Managing MC/ServiceGuard* manual.
- Data Protector Cell Manager, with recommended patches, and all other Data Protector software components for the integrations you want to have in the cluster must be installed on the Primary node and each of the Secondary nodes. See the *HP OpenView Storage Data Protector Installation and Licensing Guide* for instructions.

Configuring the Primary and Secondary Cell Managers

The following sections explain how to configure the Primary and Secondary Cell Managers.

NOTE The following sections provide step-by-step examples to configure the Primary and Secondary Cell Managers. Directory and file names, numbers, and other variables will differ from the following examples according to your environment.

Configuring the Primary Cell Manager

When configuring the Primary Cell Manager, you should first create a volume group. If you are using ob2 disk as a cluster lock disk, you should already have created a volume group for it. If you are not, follow the steps:

1. Create a volume group on a shared disk accessible to both Cell Managers (for example, `/dev/vg_ob2cm`), with the following steps:

   a. Create a directory for a new volume group:

   ```
   mkdir /dev/vg_ob2cm
   ```

NOTE The shared volume group will contain the IDB and configuration files. Keep this in mind when considering the size of the shared disk.

   b. List all existing volume groups on the system to look for the next available minor number:

   ```
   ll /dev/*/group
   ```

   c. Create a group file for the volume group:

   ```
   mknod /dev/vg_ob2cm/group c 64 0x010000
   ```

   d. Prepare the disk(s) to be used within the volume group:

   ```
   pvcreate -f /dev/rdsk/c0t1d0
   pvcreate -f /dev/rdsk/c1t2d0
   ```

   e. Create the new volume group:

   ```
   vgcreate /dev/vg_ob2cm /dev/dsk/c0t1d0 /dev/dsk/c1t2d0
   ```

2. Create a logical volume for that group (for example, `/dev/vg_ob2cm/lv_ob2cm`), with the following steps:

   a. Create a new logical volume:

   ```
   lvcreate -L 100 -n lv_ob2cm /dev/vg_ob2cm
   ```

   The number 100 presents the size of the partition in MB. The `etc/opt/omni` and `var/opt/omni` Data Protector directories will be located there.

   b. Create a journaled filesystem on the logical volume:

   ```
   newfs -F vxfs /dev/vg_ob2cm/rlv_ob2cm
   ```

NOTE If you want to mirror the new logical volume, refer to the HP-UX LVM documentation on the configuration steps.

3. Set volume group properties according to the cluster documentation, with the following steps:

   a. Deactivate the volume group from regular mode:

   ```
   vgchange -a n /dev/vg_ob2cm
   ```

   b. Mark the volume group for the cluster use:

   ```
   vgchange -c y /dev/vg_ob2cm
   ```

NOTE If this is a cluster lock disk and you are using a later version of MC/ServiceGuard like 11.09, this is done automatically.

   c. Use the volume group in the exclusive mode:

   ```
   vgchange -a e /dev/vg_ob2cm
   ```

4. Mount the logical volume to a directory (for example, `/omni_shared`), with the following steps:

   a. Create a mount point directory:

   ```
   mkdir /omni_shared
   ```

   b. Mount the filesystem to the mount point directory:

```
mount /dev/vg_ob2cm/lv_ob2cm /omni_shared
```

5. Modify the `/etc/opt/omni/sg/sg.conf` template file.

IMPORTANT

The `SHARED_DISK_ROOT` variable must contain the name of the mount point directory (for example, `SHARED_DISK_ROOT=/omni_shared`).

The `CS_SERVICE_HOSTNAME` variable must contain the name of the virtual Cell Manager, as it is known to the network. Each package in the cluster requires its own virtual IP address and its network name (for example, `CS_SERVICE_HOSTNAME=ob2cl.company.com`).

6. Configure the Primary Cell Manager. Make sure not to be positioned in the `/etc/opt/omni/` or `/var/opt/omni/` directory or their subdirectories when running the script. Make also sure to have no mounted subdirectories in the `/etc/opt/omni/` or `/var/opt/omni/`. Run:

   ```
   /opt/omni/sbin/install/omniforsg.ksh -primary
   ```

   Note that after running this script, the Data Protector services are stopped and will be restarted later on.

7. Unmount the mount point directory (Data Protector shared directory):

   ```
   umount /omni_shared
   ```

8. Deactivate the volume group you created:

   ```
   vgchange -a n /dev/vg_ob2cm
   ```

9. Export the volume group you created on the Primary Cell Manager with the following steps:

   a. From system1 (Primary Cell Manager) export the LVM configuration information with map file `/tmp/lvm_map`:

      ```
      vgexport -p -m /tmp/lvm_map /dev/vg_ob2cm
      ```

   b. Transfer the map file over to system2 (Secondary Cell Manager):

      ```
      rcp /tmp/lvm_map second_system:/tmp/lvm_map
      ```

Configuring the Secondary Cell Manager

To configure the secondary Cell Manager on system2, proceed as follows:

1. On system2 set up the volume group to be imported, with the following steps:

   a. Create a directory for the volume group to be imported:

      ```
      mkdir /dev/vg_ob2cm
      ```

   b. List all existing volume groups on the system to look for the next available minor number:

      ```
      ll /dev/*/group
      ```

   c. Create a group file for the volume group:

      ```
      mknod /dev/vg_ob2cm/group c 64 0x010000
      ```

   d. Import the volume group with map file `/tmp/lvm_map`:

      ```
      vgimport -m /tmp/lvm_map -v /dev/vg_ob2cm
      /dev/dsk/c0t1d0 /dev/dsk/c1t2d0
      ```

2. Set volume group properties according to the cluster documentation, with the following steps:

   a. Mark the volume group for the cluster use:

      ```
      vgchange -c y /dev/vg_ob2cm
      ```

NOTE If this is a cluster lock disk and you are using a later version of MC/ServiceGuard like 11.09, this is done automatically.

   b. Use the volume group in the exclusive mode:

      ```
      vgchange -a e /dev/vg_ob2cm
      ```

3. Mount the logical volume to the mount point directory, with the following steps:

   a. Create the same mount point directory as you have created on the Primary Cell Manager (`/omni_shared`):

      ```
      mkdir /omni_shared
      ```

   b. Mount the filesystem to the mount point directory:

      ```
      mount /dev/vg_ob2cm/lv_ob2cm /omni_shared
      ```

4. Configure the Secondary Cell Manager:

```
/opt/omni/sbin/install/omniforsg.ksh -secondary
/omni_shared
```

5. Unmount the mount point directory (Data Protector shared directory):

   ```
   umount /omni_shared
   ```

6. Deactivate the volume group you imported:

   ```
   vgchange -a n /dev/vg_ob2cm
   ```

Configuring the Cell Manager Package

NOTE The following section provides step-by-step examples to configure the Data Protector package. Directory and file names, numbers, and other variables will differ from the following examples according to your environment. The cluster configuration file name `cluster.conf` and the Data Protector package name `ob2cl` is used also as an example. You should follow the names given to you by your network or domain administrator.

Note that the Data Protector daemons are not running anymore on either cluster node.

Prerequisites

- The Data Protector Cell Manager should be installed and configured on both cluster nodes as explained in the previous section.
- Before configuring the Data Protector cluster package, you should have a cluster configuration file created and edited.

Configuring Data Protector Package

On the Primary Cell Manager node proceed as follows:

1. Check the cluster configuration file for errors:

   ```
   cmcheckconf -C /etc/cmcluster/cluster.conf
   ```

   If there are errors, fix them.

   If there are no errors, enable the configuration:

   ```
   cmapplyconf -C /etc/cmcluster/cluster.conf
   ```

2. Start the cluster:

   ```
   cmruncl
   ```

3. Create the directory in the `/etc/cmcluster` directory that will hold the Data Protector package:

   ```
   mkdir /etc/cmcluster/ob2cl
   ```

4. Change to the `/etc/cmcluster/ob2cl` directory:

   ```
   cd /etc/cmcluster/ob2cl
   ```

5. Create a package configuration file in the Data Protector package directory:

   ```
   cmmakepkg -p /etc/cmcluster/ob2cl/ob2cl.conf
   ```

6. Create a package control file in the Data Protector package directory:

   ```
   cmmakepkg -s /etc/cmcluster/ob2cl/ob2cl.cntl
   ```

7. Modify the Data Protector package configuration file (for example, `/etc/cmcluster/ob2cl/ob2cl.conf`). Refer to the example of this file in "Example of the Package Configuration File" on page A-28.

   In this file, modify the following fields:

Modifying the Configuration File

- `PACKAGE_NAME`

  Enter the Data Protector cluster package name. For example:

  `PACKAGE_NAME` *`ob2cl`*

- `NODE_NAME`

  Enter the names of the nodes. First enter the name of the primary (original) node, then the name(s) of the secondary node(s). For example:

  `NODE_NAME` *`partizan`*

  `NODE_NAME` *`lyon`*

- `RUN_SCRIPT`, `RUN_SCRIPT_TIMEOUT`, `HALT_SCRIPT`, `HALT_SCRIPT_TIMEOUT`

  Enter the name of the Data Protector package control file (script) and adjust the timeout for the execution of the script. By default, there is no timeout. For example:

  `RUN_SCRIPT` */etc/cmcluster/ob2cl/ob2cl.cntl/*

  `RUN_SCRIPT_TIMEOUT NO_TIMEOUT`

  `HALT_SCRIPT` */etc/cmcluster/ob2cl/ob2cl.cntl/*

  `HALT_SCRIPT_TIMEOUT NO_TIMEOUT`

- SERVICE_NAME, SERVICE_FAIL_FAST_ENABLED , SERVICE_HALT_TIMEOUT

  Enter the service information. For the service name, you can enter any name but note that you will use the same name in the control file afterwards. For example:

  ```
  SERVICE_NAME omni_sv
  SEVICE_FAIL_FAST_ENABLED NO
  SERVICE_HALT_TIMEOUT 300
  ```

- SUBNET

  Enter the subnet of the cluster. For example:

  ```
  SUBNET 10.17.0.0
  ```

8. Modify the Data Protector package control file (for example, `/etc/cmcluster/ob2cl/ob2cl.cntl`). Refer to the example of this file in "Example of the Package Control File" on page A-38.

   In this file, modify the following fields:

Modifying the Control File

- VG [n]

  Specify the volume group used by this package. For example:

  ```
  VG [0] = /dev/vg_ob2cm
  ```

- LV [n], FS [n], FS_MOUNT_OPT [n]

  Specify the logical volume and filesystem mount information:

  ```
  LV [0] = /dev/vg_ob2cm/lv_ob2cm
  FS [0] = /omni_shared
  FS_MOUNT_OPT[0]=" "
  ```

- IP, SUBNET

  Specify the IP and the subnet information used by this package. For example:

  ```
  IP [0] = 10.17.3.230
  SUBNET [0] = 10.17.0.0
  ```

- SERVICE_NAME, SERVICE_CMD, SERVICE_RESTART

  Specify the service name, command, and restart parameters.

IMPORTANT The service name must be the same as that used in the configuration file. The service command (the SERVICE_CMD variable) must be the one used in the example below.

For example:

```
SERVICE_NAME [0] = omni_sv
SERVICE_CMD [0] = "/etc/opt/omni/sg/csfailover.ksh start"
SERVICE_RESTART [0] = "-r 2"
```

To make sure that the Cell Manager package is restarted at failover, set the SERVICE_RESTART parameter to -R (to restart the service for an infinitive number of times; this is not recommended) or to "-r *<number of restarts>*" (to restart the service for defined number of times).

9. Check and propagate the Data Protector cluster package files, with the following steps:

   a. Copy the package control file to other nodes within the cluster:

   ```
   remsh system2 "mkdir /etc/cmcluster/ob2cl"
   rcp /etc/cmcluster/ob2cl/ob2cl.cntl
   system2:/etc/cmcluster/ob2cl/ob2cl.cntl
   ```

   b. Enable the Data Protector shared disk as a cluster volume group (created before) on all cluster nodes:

   ```
   vgchange -c y /dev/vg_ob2cm
   ```

   c. Check the Data Protector package:

   ```
   cmcheckconf -P /etc/cmcluster/ob2cl.conf
   ```

   d. If the check was successful, add the Data Protector package:

   ```
   cmapplyconf -P /etc/cmcluster/ob2cl.conf
   ```

   e. Start the package:

   ```
   cmrunpkg ob2cl
   ```

   The cluster should be configured and the Data Protector Cell Manager package should be up and running.

f. Import the cluster package host name manually (for example, by using the `omnicc` command):

```
omnicc -import_host <virtual_hostname> -virtual
```

g. If the Data Protector Installation Server was also installed on the MC/ServiceGuard (default), you have to import this Installation Server (for example, by using the `omnicc` command):

```
omnicc -import_is <virtual_hostname>
```

h. In order to run the Data Protector graphical user interface on the secondary node, you have to open the Data Protector graphical user interface and add the root user of the secondary node to the `admin` user group. Refer to "Adding or Deleting a User" on page 90.

Clients on MC/ServiceGuard

Data Protector can back up a full cluster (local and shared disks) and applications running in a cluster environment.

Installation

To back up a cluster-aware application, the Data Protector client must be installed locally on all the cluster nodes. See the *HP OpenView Storage Data Protector Installation and Licensing Guide* for information on how to install a cluster-aware client.

Configuration

You need to import the application cluster package to the cell.

If the Cell Manager and the application are in the same cluster, you need to move the Cell Manager package to the application node before importing the application cluster package. Proceed as follows:

1. Stop the Cell Manager package (for example `ob2cl`):

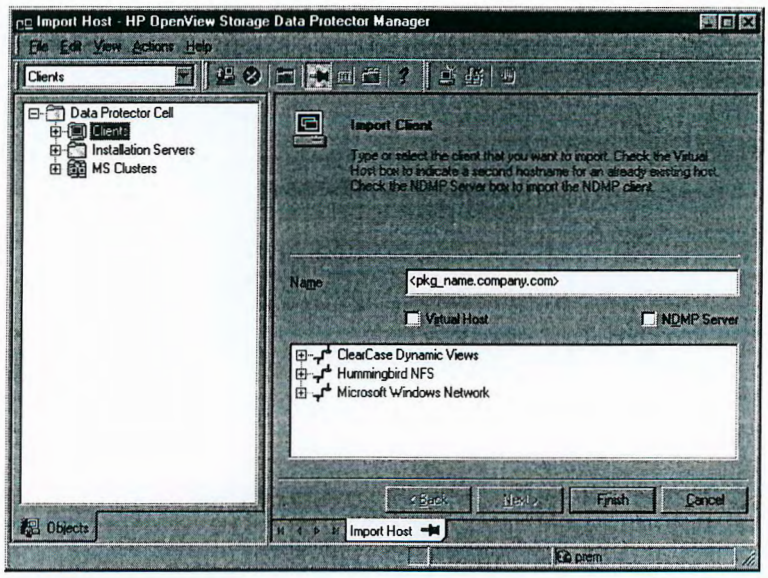
   ```
   cmhaltpkg ob2cl
   ```

2. Run the Cell Manager package on the application node:

   ```
   cmrunpkg -n <node_name> ob2cl
   ```

NOTE When using the Data Protector GUI, import each cluster package as a client. See Figure 13-4 on page 638 and the *HP OpenView Storage Data Protector Installation and Licensing Guide* for instructions.

Figure 13-4 Importing an Application Cluster Package to a Cell on MC/ServiceGuard



Backing Up Data in a Cluster (MC/SG)

This section provides an overview of how to back up specific data in a cluster environment. For additional information on backing up data in a cluster, see "Backing Up Data in a Cluster (MSCS)" on page 619.

NOTE When backing up a virtual host, the object ownership will acquire the ownership of the stationary host on which the cluster package is running. Therefore, when a failover occurs, the same object backup is showing a different ownership. To avoid this, set the ownership in the backup specification to the virtual host.

Backing Up Local Disks

To back up cluster local disks, proceed as follows:

1. Install and configure the Data Protector Disk Agent component on each cluster node that has the local disk(s) you want to back up.
2. Configure a backup specification for specific cluster node using the physical node name and select which of its local disks you want to back up.

Backing Up Shared Disks

To back up cluster shared disks, proceed as follows:

1. Install (locally) and configure the Data Protector cluster client software on all the cluster nodes. See the *HP OpenView Storage Data Protector Installation and Licensing Guide* for instructions.
2. Import cluster package to the Data Protector cell.
3. Configure a backup specification and select the virtual host. Define the shared disks you want to back up.

About Backing Up Database Applications

Information in this section is valid for backing up a database application running in the same cluster as the Cell Manager. The backup of the application fails if it runs on a different node than the Cell Manager. It is highly recommended to configure the application and the Cell Manager in the same package.

Veritas Cluster Integration

Clients on Veritas Cluster

Data Protector can only be used to back up local or shared disks in a Veritas Cluster environment.

Cluster aware operation is not supported for Data Protector with Veritas Clusters.

Installation

Data Protector has to be installed locally on each client, and each client has to be imported to the cell. See the *HP OpenView Storage Data Protector Installation and Licensing Guide* for step-by-step instructions.

To configure Veritas Cluster with Data Protector, you need the Data Protector user interface.

Refer to the following for more information:

- Veritas Cluster documentation.
- *HP OpenView Storage Data Protector Installation and Licensing Guide* for more information on how to install Data Protector.
- *HP OpenView Storage Data Protector Software Release Notes* for last minute information on the current Data Protector release.

NOTE

It is not possible to add a device on Novell NetWare virtual server.

Configuration

To be able to back up local disks on cluster nodes, the individual nodes have to be imported into the Data Protector Cell Manager.

Backing Up Local Disks

Disks local to the systems in the cluster are visible when you browse a system where a disk is locally connected.

To back up local disks:

1. Install the Data Protector Disk Agent on each system with the local disk you want to back up.
2. Configure a backup of the local system in the cluster and define the local disks you want to back up.

Backing Up Shared Disks

A shared disk can only be backed up as a local disk, as described above. It can however be backed up from any of the cluster nodes between which it is shared.

For example, to back up a disk shared between two nodes:

1. Install the Data Protector Disk Agent on each system that shares the disk.
2. Define a backup specification for the disk as a "local disk" on each system.
3. If you want to safeguard the backup of the shared disk further, you could create a post-exec within each backup specification that checks for errors and starts a backup on the other system, if the first fails.

Novell NetWare Cluster Integration

Clients on Novell NetWare Cluster

Data Protector can only be used to back up local disks or cluster shared pools in a Novell NetWare Cluster environment.

Cluster aware operation is not supported for Data Protector with Novell NetWare Clusters. In case of failover, backup or restore sessions have to be restarted manually.

Installation

Data Protector has to be installed locally on each client, and each client has to be imported to the cell. See the *HP OpenView Storage Data Protector Installation and Licensing Guide* for step-by-step instructions.

To configure Novell NetWare Cluster with Data Protector, you need the Data Protector user interface.

Refer to the following for more information:

- Novell NetWare Cluster documentation.
- *HP OpenView Storage Data Protector Installation and Licensing Guide* for more information on how to install Data Protector.
- *HP OpenView Storage Data Protector Software Release Notes* for last minute information on the current Data Protector release.

Configuration

To be able to back up local disks on cluster nodes, the individual nodes have to be imported into the Data Protector cell. To be able to back up cluster shared pools, virtual server has to be imported into the cell as well.

Backing Up Local Disks

Disks local to the systems in the cluster are visible when you browse a system where a disk is locally connected.

To back up local disks:

1. Install the Data Protector Disk Agent on each system with the local disk you want to back up.

2. Configure a backup of the local system in the cluster and define the local disks you want to back up.

Backing Up Shared Cluster Pools

A cluster shared pool can only be backed up via the virtual server. When the virtual server is selected for backup, only cluster shared pools are displayed as available pools for backup.

For example, to back up a pool shared between two nodes:

1. Install the Data Protector Disk Agent on each system that shares the pools.
2. Import the cluster virtual server into the cell.
3. Create a backup specification that includes all pools on the virtual server and start the backup.

Data Source Integration (DSI)

What Is DSI?

The Data Source Integration (DSI) allows you to use the HP OpenView Performance Agent to log data, define alarms, and access metrics from sources of data other than the metrics logged by the HP OpenView Performance Agent scopeux collector. Data Protector provides a sample script and configuration file that show you how to use the Data Protector reporting command-line interface with Data Source Integration to log data about the Data Protector environment, and backup and restore sessions.

What Can You Measure?

Some examples of what can be measured using the DSI integration are:

- Database size
- Media usage
- Media status
- Number of systems
- Amount of data per system
- Full and incremental backup figures.

Overview of Configuration

In order to use DSI, you have to:

- Identify what data you want to log
- Write a script to query data from Data Protector
- Set up a class specification file
- Compile the class specification file
- Start the logging process.

Data Protector provides a sample Korn shell (ksh) script and class specification file that, by default, log two metrics: the number of clients in cell and the size of IDB size. The script and class specification file can be easily modified for collecting other information from Data Protector. The scripts are supported on UNIX systems.

Configuring the Integration

To configure the Data Protector DSI integration, follow these steps:

1. Write a script to collect data.

First select which data you want to log. Data Protector provides a reporting command `omnirpt` located in the `/opt/omni/bin/` directory. This command can be used to gather various information about the Data Protector environment. See the `omnirpt` manpage for more information on the command. Secondly, write a script that in an infinite loop queries for the selected data and writes it to standard output.

2. Create the class specification file.

   The class specification file defines what data you want to log and how you want it to be logged. Data Protector provides a sample class specification file `obdsi.spec` in the `/etc/opt/omni/dsi` directory. Refer to the DSI manual for the complete syntax of the class specification file.

3. Compile the class specification file.

   Use the `sdlcomp` command from the `/opt/perf/bin` directory to compile the class specification file. In order to compile the Data Protector sample class specification file, use:

   ```
   sdlcomp obdsi.spec OmniBack.log OmniBack
   ```

4. Configure `perflbd.rc`

   Before you start modifying `perflbd.rc` file, you have to stop the mwa services. You do this using the following command:

   ```
   /opt/perf/bin/mwa stop
   ```

   Now you can edit the file `/var/opt/perf/perflbd.rc`. If you are configuring Data Protector sample metrics, add the following line to the file. Note that this has to be added as a single line:

   ```
   DATASOURCE=OMNIBACKII
   LOGFILE=/etc/opt/omni/dsi/OmniBack.log
   ```

5. Start the logging process.

   Start the script that collects your data and pipe its output using `dsilog` command. In case of Data Protector sample metrics, use the following command (in one line):

   ```
   obdsi.ksh | /opt/perf/bin/dsilog OmniBack.log OMNIBACKII
   ```

Application Response Measurement (ARM) Integration

What Is the ARM Integration?

Data Protector supports the emerging standard for measuring the response time of transactions in distributed environments, the Application Response Measurement (ARM) interface. Data provided by Data Protector can be used in ARM-compliant system management and monitoring tools, such as HP OpenView Performance Agent. Such tools can log this information for trend analysis, reporting, or alert-based notifications. The collected data can be viewed and analyzed by HP OpenView PerformanceManageror some other tool.

How to Install the ARM Integration

For the installation, all you need is the ARM 2.0 compatible RPM agent and the ARM 2.0-compliant library installed on the Cell Manager. It does not matter whether you install them before or after the Data Protector installation.

With a UNIX Cell Manager, you need to replace the dummy library `/opt/omni/lib/arm/libarm.sl` (HP-UX) or `/opt/omni/lib/arm/libarm.so` (Solaris) with the appropriate ARM library that actually logs transactions, or create a link to it. It is recommended to create a link. For example, in case of HP OpenView Performance Agent on an HP-UX 11.x Cell Manager, you need to link the above mentioned file to the `/opt/perf/lib/libarm.sl` file. Note that the `/opt/perf/lib/libarm.sl` file links to `libarm.0`:

Windows Cell Managers require no additional steps for setting up the ARM Integration.

What Can Be Measured?

The following information can be measured with the ARM integration:

- Overall session duration
- Disk Agent read times
- Disk Agent network write times
- Media Agent network read times
- Media Agent data write times
- Session Manager write to database time
- Database purge duration

The following table shows the supported ARM transactions:

Table 13-1 ARM Transactions

Transaction Name	Additional Information	Transaction Description
BS-<*Backup_specification*>	Time	Duration of a backup session
RS-<*Session_ID*>	Time	Duration of a restore session
BO-<*Object_name*>	Time	Duration of a backup of a specific object
DP	Number of purged records and IDB size (MB)	Duration of the IDB purge
DC	IDB size (MB)	Duration of the IDB check

ManageX Integration

What Is the ManageX Integration?

ManageX integration is supported on those Windows systems where ManageX is running. It allows the operator using ManageX to check Data Protector operation and backup status.

What Is Supported?

The integration supports the following:

- Sends the Data Protector messages with the severity levels you choose to the ManageX console.
- Checks if all Data Protector services are running and sends a messages to the ManageX console if one of the services stops.

Configuring the Integration

To configure the ManageX integration with Data Protector perform the following steps:

1. Enable Data Protector message forwarding on the Cell Manager:
   a. In the global file set `EventLogMessages=1`. Refer to "Global Options File" on page 523 for more information.
   b. Stop and restart the Data Protector services.
2. To set the Data Protector severity levels you want to receive in the ManageX console, delete or add them in the `<Data_Protector_home>\config\managex\filter` file. By default, all severity levels (`normal | warning | minor | major | critical`) are listed in this file.
3. Distribute the policies from the ManageX to Data Protector Cell Manager using the ManageX console. The Data Protector policies are in the folder Backup Applications.

Access Points for System and Management Applications

This section provides information on Data Protector access points for System and Management applications.

Introduction

The Data Protector HP OpenView Integrations allow you to administer, monitor and measure the performance of Data Protector processes using System and Application Management applications such as:

- HP OpenView Vantage Point Operations
- HP OpenView DSI
- HP OpenView ManageX

As a generic interface for these applications, Data Protector provides the following access points:

- SNMP traps
- User Interfaces (Data Protector GUI and CLI, Web reporting interface)
- Data Protector log files
- Windows Application Log

Depending on the application integrated with Data Protector, any or only some of the access points can be utilized. Data Protector already provides a set of predefined reports and actions that can be performed using the applications. They are described in the Chapter 13, "Integrations with Other Applications," on page 611.

Data Protector Access Points

SNMP Traps

SNMP traps allow a System and Application Management application to receive and process an SNMP trap message when a Data Protector event occurs or when an SNMP trap is sent as a result of Data Protector

checking and maintenance mechanism. For more information on Data Protector checking and maintenance mechanism, refer to "Data Protector Checking and Maintenance Mechanism" on page 605.

On HP-UX and Solaris, there are two Data Protector files residing on the Cell Manager, that specify the behavior of Data Protector SNMP traps:

- `/etc/opt/omni/snmp/OVdest`

  This file contains the names of the systems to receive the Data Protector SNMP traps. It has the following format:

  `trap-dest: <hostname1>`

  `trap-dest: <hostname2>`

  `...`

- `/etc/opt/omni/snmp/OVfilter`

  This file contains the severity level of the Data Protector SNMP trap messages that are to be filtered out (will not be sent by Data Protector). It has the following format:

  `<message_level>`

  `<message_level>`

  `...`

  Where `<message_level>` can be any of the following: (`normal | warning | minor | major | critical`).

On Windows systems, the destination is set in the Windows SNMP service configuration.

NOTE

On Windows systems, you need to configure the SNMP service first. For information on how to configure the Windows SNMP service, refer to "SNMP Send Method" on page 349.

The SNMP traps sent by Data Protector contain the following information:

- **Enterprise Event ID**

Each event is marked with an Enterprise Event ID (EID) used to designate the type of entity that has sent the event. The EID for the events, sent by the OpenView entity, is ".1.3.6.1.4.1.11.2.17.1".

- **Generic Event ID**

  Each event is also marked with a Generic Event ID (GID). For standard SNMP traps, the GID tells `ovtrapd` which standard SNMP trap was generated. For other types of events, the GID is **6**, meaning that the sending entity has used a Specific Event ID to further qualify the event. Data Protector uses GID 6 only.

- **Specific Event ID**

  Events with GID=6 are also marked with a Specific Event ID (SID). The use of SIDs allows enterprises to define their own custom set of event definitions. (**59047936**, used by Data Protector, is the number for the Application Alert traps which is a subtype of the existing SNMP-Traps for the HP OpenView traps.)

- **Variables**

The Table 13-2 on page 651 shows the format of SNMP traps sent by Data Protector together with exemplary values.

Table 13-2 Data Protector SNMP Traps Format

MIB ID	Meaning	Exemplary Value
1.3.6.1.4.1.11.2.17.1.1.0	Application type	1
1.3.6.1.4.1.11.2.17.1.2.0	Hostname of the Cell Manager	machine.company.com
1.3.6.1.4.1.11.2.17.1.3.0	Trap message type	Either NOTIFICATION or nothing
1.3.6.1.4.1.11.2.17.1.4.0	Application name	HP Data Protector
1.3.6.1.4.1.11.2.17.1.5.0	Severity of the message	critical
1.3.6.1.4.1.11.2.17.1.6.0	The message	Error on device "DLT_1" occurred
1.3.6.1.4.1.11.2.17.2.7.0	Parameter list	Mount request for device name=DLT_1

Command-Line Interface, Graphical User Interface and Web Reporting Interface

The Data Protector CLI provides comparable functionality as it is provided in Data Protector GUI. Using the Data Protector CLI you can:

- Start the Data Protector GUI and sub-GUIs. For a list of the Data Protector sub-GUIs, refer to "Graphical User Interface" on page 6.
- Configure and start Data Protector actions such as backup, restore and IDB purge. For a list of possible Data Protector actions, refer to Appendix, "Data Protector Commands," on page A-7.
- Configure and start Data Protector reports using the Data Protector `omnirpt` CLI command. For more information about reporting, refer to "Data Protector Reporting" on page 315.
- Start the Java user interface to configure and start Data Protector reports. For more information about web reporting, refer to "Configuring Reports and Notifications on the Web" on page 353.

You can use Data Protector commands for scripts that provide the input data to System and Application Management application.

Data Protector Log Files

Some System and Application Management applications, such as HP OpenView Vantage Point Operations, allow you to specify when and which log files should be monitored for a specific log entry. If the specified entry is detected in the file, an action can be specified. In VPO this is called *Log file encapsulation*.

You can configure such a System and Application Management application to monitor Data Protector log files for specific log entries (Data Protector events) and define an action that is to be executed in case a particular Data Protector event is detected.

For more information on Data Protector log files refer to "Data Protector Log Files" on page 550. Note that there is no log files formatting specification provided. For Data Protector log files exemplary entries, refer to Appendix, "Data Protector Log Files Example Entries," on page A-44.

Windows Application Log

Some System and Application Management applications, such as ManageX, monitor the Windows Application Log.

To enable automatic forwarding of all Data Protector messages and messages about the Data Protector services (if they are stopped) to Windows Application Log, set the `EventLogMessages` variable in the Data Protector global options file to `1`. For more information on Data Protector global options file refer to "Global Options File" on page 523.

Examples

Verifying Data Protector Processes

Data Protector provides a means of checking if its required processes are running by the means of the `omnisv -status` CLI command.

The `omnisv -status` command provides you with the status of the required Data Protector processes (when the command is started).

omnisv -status

To get the status of required Data Protector processes enter the following command:

```
omnisv -status
```

Data Protector Health Check Failed Notification

The User Health Check notification is triggered and sent only if any of the required processes are not running or if the IDB is not operational. The Health Check Failed notification by default checks these conditions every day at 12:00 (Noon) and is (if the conditions are met), by default sent to Data Protector Event Log. You can change the scheduled time by changing the `DailyMaintenanceTime` variable, using the twenty-four hour clock notation, in the Data Protector global options file. For more information on Data Protector global options file refer to "Global Options File" on page 523. You can also redirect the notification to be sent, for example as an SNMP trap.

To check every day at the scheduled time if the required Data Protector processes are running and if the IDB is operational, and to be notified by an SNMP trap if any of the processes are not running or if database is not operational, configure the Health Check Failed notification as described in the "Data Protector Notifications" on page 342.

To check the conditions of the Health Check Failed notification interactively, enter the following command:

```
omnihealthcheck
```

Refer to the `omnihealthcheck` man page for more information on `omnihealthcheck` command.

Getting the Results of the Last Night's Backup

You can get the report on the results of the last night's backups using the Data Protector reporting functionality. For more information on Data Protector reporting functionality refer to "Data Protector Reporting" on page 315 and to the `omnirpt` man page - more than 30 different reports, each having many different options, can be run.

To get the HTML report on the last night's backup in the file `report.html` enter the following command:

```
omnirpt -report list_sessions -timeframe 24 24 -html -log
report.html
```

14 ADIC/GRAU DAS and STK ACS Libraries

In This Chapter

This chapter assumes that you have already physically configured the ADIC/GRAU or STK library. If you have not done so, refer to the documentation that comes with the ADIC/GRAU or STK library for instructions on configuring the library. For a list of supported DAS software versions, refer to *HP OpenView Storage Data Protector Software Release Notes*.

This chapter has been divided into three sections: an overview of general concepts, the ADIC/GRAU DAS library, and the STK ACS library. The first section covers concepts common to both libraries, including diagrams of both library configurations with Data Protector, and media management basics. The next section provides detailed instruction on installing and configuring the ADIC/GRAU library, and the last section provides detailed instruction on installing and configuring the STK ACS library. The ADIC/GRAU and STK library sections are structured in the following order:

"ADIC/GRAU DAS and STK ACS Integrations" on page 657.

"The ADIC/GRAU DAS Library Device" on page 662.

"The STK ACS Library Device" on page 680.

"Troubleshooting Library Installation and Configuration" on page 697.

NOTE The ADIC/GRAU and STK functionality is subject to specific Data Protector licenses. See the *HP OpenView Storage Data Protector Installation and Licensing Guide* for details.

ADIC/GRAU DAS and STK ACS Integrations

Who Uses the ADIC/GRAU DAS or STK ACS Integration?

Typically, the Data Protector and ADIC/GRAU DAS or STK ACS integration is necessary in complex environments where the amount of backed up data is exceptionally large and, therefore, so is the amount of media needed to store the data. The ADIC/GRAU and STK libraries are not only capable of managing large amounts of media, they are also capable of managing media used by different applications, not just Data Protector.

Data Protector provides full support for the ADIC/GRAU DAS and the STK ACS Library Systems. Since these libraries manage media used by different applications, you have to configure which media you want to use with Data Protector, which media you want to track, and which drives you want to use with Data Protector. The following diagrams represent the two library integrations:

Figure 14-1 **Data Protector and ADIC/GRAU DAS Library Systems Integration**

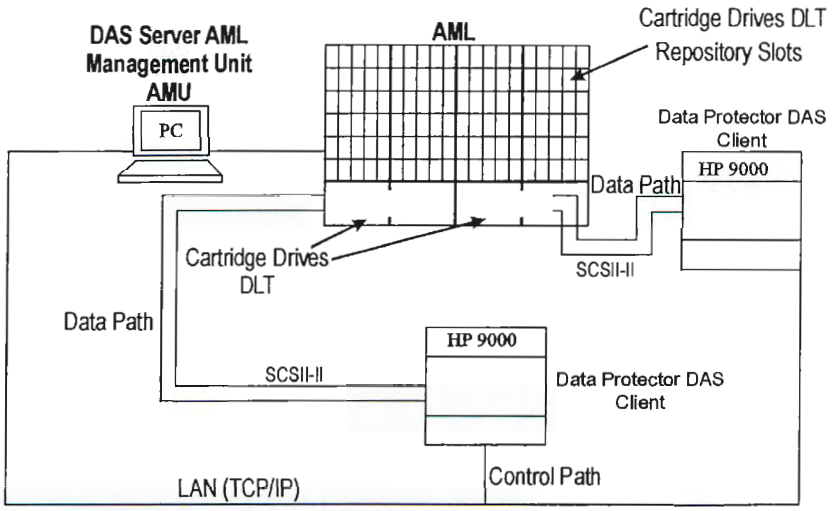
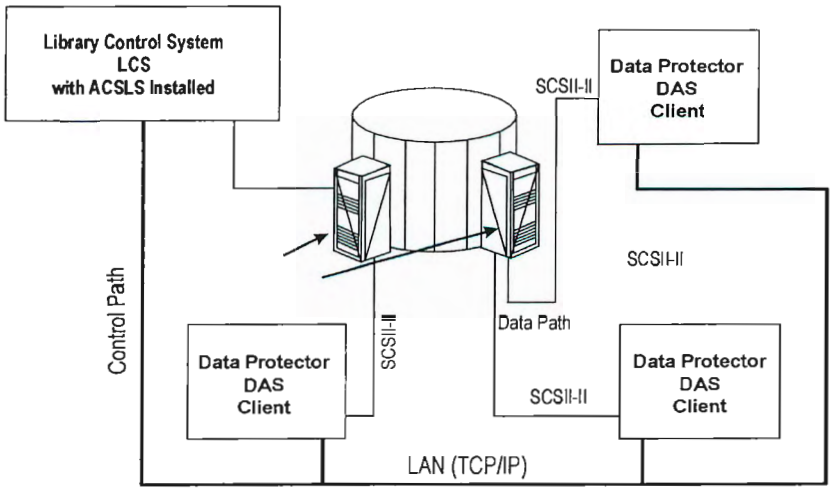


Figure 14-2 **Data Protector and StorageTek ACS Library Integration**



Configuration Basics

When considering your environment and the configuration that is best for you, keep in mind that there are two ways to configure the ADIC/GRAU and STK ACS libraries with Data Protector: where each client accesses the library directly (direct access to the library), or where each client is connected to one system that controls the library robotics through the server (indirect access to the library). Regardless of the configuration you choose, direct or indirect, the DAS or ACS Media Agent software has to be installed on each client that directly or indirectly accesses the library robotics. For the ADIC/GRAU integration, each system on which you install the DAS Media Agent software is called a *DAS Client*. For the STK ACS integration, each system on which you install the ACS Media Agent software is called an *ACS Client*.

Choosing the Direct or Indirect Library Access Configuration

The direct library access configuration is recommended and, with previous versions of Data Protector, it was the only possible configuration. When either DAS or ACS Client has direct access to the library, there is no chance of single point of failure. That is, with the indirect access configuration, if the client with direct access to the library fails, all the clients that access the library through that system also lose access to the library.

Media Management Basics

In the ADIC/GRAU DAS and STK ACS library devices, the size of the repository with media depends on your license. A medium is identified by its volume serial number, or volser. The volser, similar to a barcode, uniquely identifies each medium during its life.

Media in the library can be used by many applications, not just by Data Protector, so that you have to know which applications use which media to prevent them from being overwritten.

Ideally, you will use the ADIC/GRAU or ACS library with Data Protector exclusively and let Data Protector manage the complete library, but if you have other applications using the library, you should take care to assign non-intersecting subsets of media to Data Protector and other applications. Also, note that Data Protector does not make use of scratch pools but maintains its own independent media allocation policy. This implies that if a specific medium has been allocated to Data Protector

(added to an Data Protector media pool), it remains under Data Protector's control during its lifetime or until it is removed from the Data Protector media pool.

IMPORTANT

Each type of media has to have its own library. While the ADIC/GRAU or STK ACS system can store many physically different types of media, Data Protector can only recognize a library with a single type of media in it. Therefore you have to create a Data Protector library for every media type in the DAS system.

The actual physical location of a medium is maintained by the DAS Server (in the ADIC/GRAU library) or the ACS Server (in the STK ACS library), not Data Protector. The DAS or ACS Server tracks the location using its volser. When a medium is moved around the repository, it is not assigned to the same physical slot each time. Therefore, you cannot rely on the slot number when handling the media, but on the barcode (volser).

For media in the device's repository, Data Protector displays the location as **resident**. For media stored outside the device's repository, Data Protector displays the location as **non-resident**.

NOTE

Data Protector will not overwrite media containing data in a recognizable format. However, Data Protector can not guarantee that Data Protector data on tapes will not be overwritten by some other application using the same media. We recommend that you make sure that media used by Data Protector are not used by any other application, and vice versa.

Tracking Media

Data Protector tracks both Data Protector and non-Data Protector media. For media in a recognizable format, Data Protector displays the format as the media type, such as **tar**. For media in a non-recognizable format, Data Protector displays **foreign** as the media type.

Labeling Media

Data Protector labels each medium used by Data Protector with the unique medium label and medium ID. Both are stored in the IDB and allow Data Protector to manage the medium. The medium ID is assigned by Data Protector, while the medium label is combined from your description and the volser of this medium.

Although you can change the label and exclude the barcode number, this is not recommended. In this case you should manually keep track of the actual barcode and the medium label you assigned to the medium.

Initializing Other Formats

If Data Protector recognizes some other media data format or media that have been used by another application, it will not initialize these media unless the `Force Operation` option is selected. Data Protector recognizes the following data formats and media used by other applications: tar, cpio, Fbackup, FileSys, Ansi and OmniStorage.

Drive Cleaning Support

The ADIC/GRAU DAS and STK ACS libraries can automatically clean their drives after the drive has been used a set number of times. This is not recommended, as library built-in drive cleaning interrupts the session, causing it to fail. If you want to use the library's cleaning functionality, you have to ensure that drive cleaning is performed when no Data Protector sessions are running.

For more information on drive cleaning methods, refer to "Drive Cleaning" on page 61.

Additional Media Management Tips

Remember the following list of tips when you begin to use Data Protector with the GRAU DAS or STK ACS device.

- Create at least one media pool for each media type, for example, one for 4mm and one for 3480 media type. Depending on your environment, you may want to create more media pools, for example, one for each department. See *HP OpenView Storage Data Protector Concepts Guide* for more information on how to plan your media pools.
- Use Data Protector commands to handle media. If you handle media manually using ADIC/GRAU DAS or STK ACS commands, Data Protector will not be able to track the changes in location or information on the media.
- Manage the whole library with Data Protector. This provides single-point administration where you can track Data Protector and non-Data Protector media in the library.
- Make sure that Data Protector and other applications do not use the same set of media.

The ADIC/GRAU DAS Library Device

Data Protector provides full support for the ADIC/GRAU DAS Library Systems. This section describes how you install and configure ADIC/GRAU DAS library devices for direct and indirect library access.

Direct Access to the Library: Installation and Configuration

This section focuses on the direct access configuration. The section is structured in the following order:

- Initial steps you have to complete to prepare for installation
- How to install the DAS Media Agent software on Windows, HP-UX, and AIX platforms
- Configuring the ADIC/GRAU library using the Data Protector GUI
- Configuring drives using the Data Protector GUI
- Accessing the ADIC/GRAU library using the Data Protector GUI

Connecting Library Drives

Physically connect the library drives and robotics to the systems where you intend to install the DAS Media Agent software.

See http://www.openview.hp.com/products/datapro/spec_0001.html for details about supported ADIC/GRAU libraries.

See "Installing the HP-UX Client System" in the *HP OpenView Storage Data Protector Installation and Licensing Guide* for information on how to physically attach a backup device to a UNIX system.

See "Installing the Windows Client System" in the *HP OpenView Storage Data Protector Installation and Licensing Guide* for information on how to physically attach a backup device to a Windows system.

Preparing for Installation

The following steps pertain to configuring the ADIC/GRAU library, and should be completed before you install the DAS Media Agent software:

- Before you configure a Data Protector ADIC/GRAU backup device, you have to create/update the `C:\DAS\ETC\CONFIG` file on the DAS server computer. In this file, a list of all DAS clients has to be defined. For Data Protector, this means that each Data Protector client with the DAS Media Agent installed has to be defined.

  Each DAS client is identified with a unique client name (no spaces), for example DATA_PROTECTOR_C1. In this example, the contents of the `C:\DAS\ETC\CONFIG` file should look like this:

  ```
  client  client_name = DATA_PROTECTOR_C1,
  #       hostname = AMU,"client1"
          ip_address = 19.18.17.15,
          requests = complete,
          options = (avc,dismount),
          volumes = ((ALL)),
          drives = ((ALL)),
          inserts = ((ALL)),
          ejects = ((ALL)),
          scratchpools = ((ALL))
  ```

  These names have to be configured on each Data Protector DAS Media Agent client as the `omnirc` variable `DAS_CLIENT`. The `omnirc` file is either the `omnirc` (on Windows) on the Data Protector home directory or the `.omnirc` file (on UNIX). For example, on the system with the IP address 19.18.17.15, the appropriate line in the `omnirc` file is DAS_CLIENT=DATA_PROTECTOR_C1.

- You have to find out how your GRAU library slot allocation policy has been configured, either statically and dynamically.

  The static policy has a designated slot for each volser while the dynamic allocation policy assigns the slots randomly. Depending on the policy that has been set, however, you need to configure Data Protector accordingly.

  If the static allocation policy has been configured, you need to add the following `omnirc` variable to your system controlling the robotics of the library:

  ```
  OB2_ACIEJECTTOTAL = 0
  ```

NOTE This applies to HP-UX and Windows.

For further questions on the configuration of your GRAU library please contact your local GRAU support or review your GRAU documentation.

Installing the DAS Media Agent

Data Protector provides a dedicated ADIC/GRAU library policy used to configure an ADIC/GRAU library with Data Protector. You have to install the Data Protector DAS Agent component on every system that will be physically connected to a drive in the ADIC/GRAU library.

NOTE You need special licenses, depending on the number of drives and slots used in the ADIC/GRAU library. See "Data Protector Licensing" in the *HP OpenView Storage Data Protector Installation and Licensing Guide* for more information.

DAS Agent includes standard Media Agent functionality, thus the Media Agent must not be installed over an existing DAS Agent.

Installing the DAS Media Agent on a Windows System

Prerequisites The following prerequisites for installation have to be met before installing DAS Agent on a Windows system:

- The ADIC/GRAU library has to be configured and running. See the documentation that comes with the ADIC/GRAU library.
- Data Protector has to be installed and configured. See "Installing the Cell Manager (CM) and Installation Server (IS)" in the *HP OpenView Storage Data Protector Installation and Licensing Guide* for more information.
- The following information has to be obtained before you install DAS Agent:
  - ✓ A hostname of the DAS Server (an application that runs on OS/2 host).

✓ A list of available drives with corresponding DAS name of the drive.
If you have defined the DAS Clients for your ADIC/GRAU system, you can get this list with the following `dasadmin` commands:

`dasadmin listd2 [client]` or

`dasadmin listd [client]`, where `[client]` is the DAS Client for which the reserved drives are to be displayed.

`Dasadmin` command can be called from the `C:\DAS\BIN` directory on the OS\2 host, or from the system directory: `\winnt\system32`

✓ A list of available Insert/Eject Areas with corresponding format specifications.
You can get the list of available Insert/Eject Areas in Graphical configuration of AMS (AML Management Software) on OS\2 host:

1. Start this configuration from the menu `Admin -> Configuration`.
2. Open the `EIF-Configuration` window by double-clicking the I/O unit icon, and then click the `Logical Ranges` field.
   In the text box the available Insert/Eject Areas are listed.

NOTE

One Data Protector library device can handle only one media type.
It is important to remember which media type belongs to each one of the specified Insert and Eject Areas, because you will need this data later for configuring Insert/Eject Areas for the Data Protector library.

✓ A list of SCSI addresses for the drives. For example, scsi4:0:1:0.

Remote Installation

The installation procedure consists of these steps:

1. Distribute the DAS Agent component to clients using the Data Protector graphical user interface and Installation Server.
2. Physically connect the library drives and robotics to the systems where you have installed the DAS Agent software.

   See http://www.openview.hp.com/products/datapro/spec_0001.html for details about supported ADIC/GRAU libraries.

At this stage, you should have your hardware connected and your DAS software properly installed. Run the following command to check whether or not the library drives are properly connected to your system:

- `<Data_Protector_home>\bin\devbra -dev`

You should see the library drives with corresponding device files displayed in the list.

For the NT platform, install the ADIC/GRAU library for client interface `aci.dll`, `winrpc32.dll` and `ezrpcw32.dll` libraries to the `<Data_Protector_home>\bin` directory. Copy these three libraries to `winnt\system32` directory as well. Copy `Portinst` and `Portmapper service` to the DAS Client. (Customer gets these requirements with the ADIC/GRAU library on a special driver installation diskette). Start `portinst` to install `portmapper`. The DAS Client needs to be rebooted to start the `portmapper service`. After reboot check if `portmapper` and both `rpc services` are running: in the Windows Control Panel, go to `Services` (Windows NT) or `Administrative Tools, Services` (other Windows systems).

Installing the DAS Media Agent on a 32-bit HP-UX System

Prerequisites

The following prerequisites for installation have to be met before installing DAS Agent on a 32-bit HP-UX system:

- The ADIC/GRAU library has to be configured and running. See the documentation that comes with the ADIC/GRAU library.
- Data Protector has to be installed and configured. See "Installing the Cell Manager (CM) and Installation Server (IS)" in the *HP OpenView Storage Data Protector Installation and Licensing Guide* for more information.
- The following information has to be obtained before you install DAS Agent:
  - ✓ A hostname of the DAS Server (an application that runs on OS/2 host).
  - ✓ A list of available drives with corresponding DAS name of the drive.
    If you have defined the DAS Clients for your ADIC/GRAU system, you can get this list with the following `dasadmin` commands:

    `dasadmin listd2 [client]` or

`dasadmin listd [client]`, where `[client]` is the DAS Client for which the reserved drives are to be displayed.

`Dasadmin` command can be called from the `C:\DAS\BIN` directory on the OS\2 host, or from the system directory: `/usr/local/aci/bin` directory.

✓ A list of available Insert/Eject Areas with corresponding format specifications.
You can get the list of available Insert/Eject Areas in Graphical configuration of AMS (AML Management Software) on OS\2 host:

1. Start this configuration from the menu `Admin -> Configuration`.
2. Open the `EIF-Configuration` window by double-clicking the I/O unit icon, and then click the `Logical Ranges` field.
   In the text box the available Insert/Eject Areas are listed.

NOTE

One Data Protector library device can handle only one media type. It is important to remember which media type belongs to each one of the specified Insert and Eject Areas, because you will need this data later for configuring Insert/Eject Areas for the Data Protector library.

✓ A list of UNIX device files for the drives.

Run the `ioscan -fn` system command on your system to display the required information.

Remote Installation

The installation procedure consists of these steps:

1. Distribute the DAS Agent component to clients using the Data Protector graphical user interface and Installation Server.
2. Physically connect the library drives and robotics to the systems where you have installed the DAS Agent software.

   See http://www.openview.hp.com/products/datapro/spec_0001.html for details about supported ADIC/GRAU libraries.

At this stage, you should have your hardware connected and your DAS software properly installed. Run the following command to check whether or not the library drives are properly connected to your system:

- `/opt/omni/lbin/devbra -dev`

You should see the library drives with corresponding device files displayed in the list.

For the HP-UX platform, install the ADIC/GRAU library for client interface:

Copy `libaci.sl` shared library into the `/opt/omni/lib` directory.

Installing the DAS Media Agent on an AIX System

Prerequisites

The following prerequisites for installation have to be met before installing DAS Agent on an AIX system:

- The ADIC/GRAU library has to be configured and running. See the documentation that comes with the ADIC/GRAU library.
- Data Protector has to be installed and configured. See "Installing the Cell Manager (CM) and Installation Server (IS)" in the *HP OpenView Storage Data Protector Installation and Licensing Guide* for more information.
- The following information has to be obtained before you install DAS Agent:
  - ✓ A hostname of the DAS Server (an application that runs on OS/2 host).
  - ✓ A list of available drives with corresponding DAS name of the drive.
    If you have defined the DAS Clients for your ADIC/GRAU system, you can get this list with the following `dasadmin` commands:

    `dasadmin listd2 [client]` or

    `dasadmin listd [client]`, where `[client]` is the DAS Client for which the reserved drives are to be displayed.

    `Dasadmin` command can be called from the `C:\DAS\BIN` directory on the OS\2 host, or from the system directory: `/usr/local/aci/bin` directory
  - ✓ A list of available Insert/Eject Areas with corresponding format specifications.
    You can get the list of available Insert/Eject Areas in Graphical configuration of AMS (AML Management Software) on OS\2 host:

    1. Start this configuration from the menu `Admin -> Configuration`.

2. Open the `EIF-Configuration` window by double-clicking the I/O unit icon, and then click the `Logical Ranges` field. In the text box the available `Insert/Eject` Areas are listed.

NOTE

One Data Protector library device can handle only one media type. It is important to remember which media type belongs to each one of the specified Insert and Eject Areas, because you will need this data later for configuring Insert/Eject Areas for the Data Protector library.

Run the following system command to check whether or not the library drives are properly connected to your system:

```
lsdev -C
```

You should see your device listed.

Remote Installation

The installation procedure consists of these steps:

1. Distribute the DAS Agent component to clients using the Data Protector graphical user interface and Installation Server.
2. Physically connect the library drives and robotics to the systems where you have installed the DAS Agent software.

   See http://www.openview.hp.com/products/datapro/spec_0001.html for details about supported ADIC/GRAU libraries.

At this stage, you should have your hardware connected and your DAS software properly installed.

For the AIX platform, install the ADIC/GRAU library for client interface:

Copy `libaci.o` shared library into the *<Data_Protector_home>*`/lib` directory.

Using the Data Protector GUI

Configure the ADIC/GRAU library the DAS client of which will access ADIC/GRAU robotics during specific Media Management operations (Query, Enter, Eject). The steps are as follows:

- In the `HP OpenView Storage Data Protector Manager` switch to the `Devices & Media` context. In the Scoping Pane, right-click `Devices` and then click `Add Device`.

- Enter the Device Name and, below, Description.
- In the Client text box choose the DAS Media Agent client from the list that will access ADIC/GRAU robotics.
- Choose the GRAU DAS Library in the Device type text box. In the DAS Server enter the hostname of the DAS Server (obtained information during installing DAS Agent).
- Choose preferred action from the list for the Busy Drive situation. Insert the Import and Export Areas for the media type this Data Protector library is configured for (obtained information during installing DAS Agent).
- Choose appropriate Media Type from the list.

Using Data Protector to Configure Drives

Create a library for each type of media that you will use with Data Protector. The steps to add a drive to a ADIC/GRAU library are as follows:

- Switch to the Devices & Media context. Choose created device, right-click Drives, and then Add Drive. Enter the Device Name and Description.
- In the Client text box enter the hostname where the ADIC/GRAU media device is connected.
- In Data Drive enter the SCSI address of the device.
- In the Drive Name enter the ADIC/GRAU Drive name you remembered during installing the DAS Agent. Select the appropriate Media Pool you created for this Drive.
- Select Advanced Options to change Concurrency and other settings as necessary. Note that the Force Direct Library Access option is not selected by default. Turn this option off when choosing the indirect library robotics access configuration (for more information, see the following section, "Indirect Access to the DAS Library: Installation and Configuration").

Indirect Access to the DAS Library: Installation and Configuration

This section focuses on the indirect access configuration.

Configuring the indirect access platform requires the same preparatory steps as configuring the direct access platform. You have to create a DAS Client in the `C:\DAS\ETC\CONFIG` file on the DAS Server computer, install the ADIC/GRAU library in the Data Protector `/bin` directory, and install and start the Portmapper service. Detailed instructions are provided in "Preparing for Installation" in the preceding section, "Direct Access to the Library Robotics: Installation and Configuration."

Using Data Protector to Configure the ADIC/GRAU Library and Drives

The indirect access configuration steps are the same as the direct access configuration (see previous section for steps), except the default setting, `Force Direct Library Access`, should be turned off.

- Follow the same GUI steps as for the direct library access configuration. When the library configuration is complete, you will be prompted to create library drives.
- Follow the same steps for creating drives as in the indirect library access configuration, but in `Advanced Options`, make sure to turn off the `Force Direct Library Access` feature. By default, this feature is off.

Using Data Protector to Access the ADIC/GRAU Library

Once you have configured your environment and installed the DAS Media Agent on the systems that will access the library robotics, you are ready to use the Data Protector GUI to access the media in the ADIC/GRAU DAS library. The following sections provide instructions on using Data Protector with the ADIC/GRAU integration.

Searching for a Medium

Use this function to locate a specific medium without having to browse the entire list of media. Data Protector locates media by searching through media, then Medium Locations, and finally Medium IDs.

1. In the `HP OpenView Storage Data Protector Manager`, switch to the `Devices & Media` context.
2. To search for media in a media pool, select the `Media` item.

   To search for media in a library, select the `Devices` item.

3. In the `Edit` menu, click `Find`. The Find dialog box appears.

   Use the appropriate search method to search for media.

Entering Media

Use this functionality to physically enter media into an ADIC/GRAU DAS repository and automatically register added media as members of the library.

1. In the `HP OpenView Storage Data Protector Manager`, switch to the `Devices & Media` context.
2. In the Scoping Pane, click `Devices`. The list of configured devices will display in the Results Area.
3. In the list of configured devices, click the name of the library, then expand it to display the `Drives` and `Slots` items.
4. Click `Slots` to display the list of slots in the Results Area.
5. Right-click the slot where you want to enter the medium, and then click `Enter`.

   See online Help for further information.

Ejecting Media

Use this functionality to physically move selected media from the repository into an Insert/Eject area.

1. In the `HP OpenView Storage Data Protector Manager`, switch to the `Devices & Media` context.
2. In the Scoping Pane, click `Devices`. The list of configured devices will display in the Results Area.
3. In the list of configured devices, click the name of the library, then expand it to display the `Drives` and `Slots` items.
4. Click `Slots` to display the list of slots in the Results Area.
5. Right-click the slot from which you want to eject the medium, and then click `Eject Medium`.

   See online Help for further information.

Adding Media to a Media Pool

Adding media to a media pool registers the new media in the IDB as members of this media pool. It is not necessary for these media to actually reside in the DAS repository.

To add media to a pool, you have to first initialize them. Initializing media prepares it for use with Data Protector. See "Initializing Media." You can also import it. See "Importing Media."

Initializing Media

Initializing media prepares media for use with Data Protector by saving the information about the media (medium ID, description and location) in the IDB and also writes this information on the medium itself (media header). When you initialize media, you also specify to which media pool the media belong.

You need to initialize media before you use media for backup. If media are not initialized before backup, Data Protector formats media during backup. This increases the backup time.

Initializing Individual Media

1. In the `HP OpenView Storage Data Protector Manager`, switch to the `Devices & Media` context. Right-click the desired device.
2. Expand the `Media` item, right-click the desired media pool, and then select `Format`. The `Format` wizard appears.
3. Select the device (library's drive and slot) where the medium to format is located. Click `Next`.
4. Specify the description and location for the new medium.

   Under `Medium Description`, either have Data Protector `Automatically Generate` a name for the medium, or click the `Specify` radio button and enter a name for the medium in the accompanying text box.

   In the `Location` drop-down list, specify where you keep the medium, after it is removed from the library. Click `Next`.
5. Specify additional options for the session.

   The `Force Operation` button will automatically initialize blank media or media in other formats recognized by Data Protector (tar, cpio, OmniBackI, and so on). You can leave the default. Data Protector media containing protected data will not be re-initialized even if this option is set.

The Medium Size button decides whether Data Protector will Determine the storage size of the medium, or whether you want to Specify the storage size of the medium. You can leave the default, which is Determine. Click Finish.

TIP Follow online Help for information on the format wizard.

Initializing Multiple Media in a Library Device

1. In the HP OpenView Storage Data Protector Manager, switch to the Devices & Media context.
2. Under Devices, expand the library device that contains the media that you want to initialize.
3. Expand the Slots item, and then select a range of slots to initialize.

   Right-click the selected range of slots, and then select Format. The Format wizard appears.
4. In the Destination page, in the Media Pool drop-down box, select the media pool to which the media will be assigned.
5. Click Next. The Medium Name page appears.
6. Under Medium Name, either have Data Protector Automatically Generate a name for the medium, or click the Specify radio button and enter a name for the medium in the accompanying text box.
7. In the informational User Location drop-down box, either enter or select the location of the media's user.
8. Click Next. The Initializing Options page appears.
9. Optionally, use the Medium Capacity button to define whether Data Protector will Determine the storage size of the medium, or whether you want to Specify the storage size of the medium. You can leave the default, which is Determine.
10. Optionally, using the Force Initialization button will automatically initialize blank media or media in other formats recognized by Data Protector (tar, cpio, OmniBackI, and so on). You can leave the default. Data Protector media containing protected data will not be re-initialized even if this option is set. The Eject option, if set, will eject a medium from the drive after the initialization completes.

Follow online Help for information on specific items in the wizard.

11. Click `Finish` to confirm and exit the wizard.

Querying the ADIC/GRAU DAS Server

If you want to get information about a repository in the GRAU DAS library from the Server, you can query the DAS Server. A query responds with the contents of the media database of the DAS Server, and then synchronizes the information in the IDB with what is actually in the repository.

This is especially useful if you were using GRAU DAS commands to manage media, as this results in inconsistencies with the IDB - Data Protector does not know the latest status of media in the library repository. Proceed as follows:

1. In the `HP OpenView Storage Data Protector Manager`, switch to the `Devices & Media` context.
2. In the list of configured devices, right-click the library you want to query, then click `Query`.

   See online Help for further information.

This action queries the DAS Server for information.

Verifying Media

Use this function to verify media in a media pool. By reading all media blocks and parsing all the headers, then parsing all Media Agent blocks and checking records in each block, Data Protector determines whether the data on the media is valid. If the `CRC` option was set during backup, Data Protector recalculates the CRC and compares the values.

You can only verify resident Data Protector media.

1. In the `HP OpenView Storage Data Protector Manager`, switch to the `Devices & Media` context.
2. In the Scoping Pane, click `Devices`. The list of configured devices will display in the Results Area.
3. In the list of configured devices, click the name of the library, then expand it to display the `Drives` and `Slots` items.
4. Click `Slots` to display the list of slots in the Results Area.
5. Select a range of slots to verify.

6. Right-click your selected slots and their media, and then click `Verify`.

   See online Help for further information.

Scanning Media

Use this function to examine the format of selected media. Also see "Scanning Media in a Device" on page 129 for more information.

1. In the `HP OpenView Storage Data Protector Manager`, switch to the `Devices & Media` context.
2. In the Scoping Pane, click `Devices`. The list of configured devices will display in the Results Area.
3. In the list of configured devices, click the name of the library, then expand it to display the `Drives` and `Slots` items.
4. Click Slots to display the list of slots in the Results Area.
5. Select a range of slots to scan.
6. Right-click your selected slots and their media, and then click `Scan`.

   See online Help for further information.

When the scan process has been completed, the `Library Management` window is updated with information on the format of the examined media.

Modifying Media Attributes

Use this function to change the location or label description of Data Protector media. For example, you would want to change the location of a medium when the medium is sent to offsite storage.

1. In the `HP OpenView Storage Data Protector Manager`, switch to the `Devices & Media` context.
2. In the Scoping Pane, click `Devices`. The list of configured devices will display in the Results Area.
3. In the list of configured devices, click the name of the library, then expand it to display the `Drives` and `Slots` items.
4. Click `Slots` to display the list of slots in the Results Area.
5. Select a slot and its resident medium to modify.

6. Change the information that appears in the Results Area.

   See online Help for further information.

NOTE These modifications are made to the IDB, and not to the tape itself.

Moving Media

Use this function to move media from one media pool to another. When you move media to another media pool, all the media information such as condition, type, medium ID, and session information is transferred to the new media pool.

Getting Information about Media

Use this functionality to display detailed information about the usage and condition of an individual selected Data Protector medium. *This is a read-only window.*

1. In the `HP OpenView Storage Data Protector Manager`, switch to the `Devices & Media` context.
2. In the Scoping Pane, click `Devices`. The list of configured devices will display in the Results Area.
3. In the list of configured devices, click the name of the library, then expand it to display the `Drives` and `Slots` items.
4. Click `Slots` to display the list of slots in the Results Area.
5. Select a slot and its resident medium to view.
6. Information about the media appears in the Results Area.

   See online Help for further information.

Recycling Media

Recycling a Data Protector-owned medium removes protection from data objects contained on the medium. Recycled media can be reused for backup. Also see "Recycling Media" on page 123 for more information.

1. In the `HP OpenView Storage Data Protector Manager`, switch to the `Devices & Media` context.

2. In the Scoping Pane, click Devices. The list of configured devices will display in the Results Area.
3. In the list of configured devices, click the name of the library, then expand it to display the Drives and Slots items.
4. Select and then right-click the slots that you want to recycle.
5. Click Recycle.

   See online Help for further information.

Removing Volsers

This action does not affect volsers in the GRAU DAS library but only removes specific media from the IDB. Therefore, Data Protector does not know that these media exist and does not use them.

1. In the HP OpenView Storage Data Protector Manager, switch to the Devices & Media context.
2. Under Devices, expand the device that has the media that you want to remove.
3. Expand the Slots item and select the slots that you want to remove.
4. In the Actions menu, click Delete. The confirmation dialog box appears for you to confirm that you want to remove the selected media.
5. Click OK to remove the selected media.

NOTE

If the number of media to be removed exceeds more than fourteen in one go, the media will not be referred to by ID (displayed in the window). You will simply be asked if you wish to remove that amount of media, for example, 22 media.

Exporting Media

This functionality enables you to remove information about backup objects contained on Data Protector media from the IDB. Use it when media will no longer be used in a Data Protector cell. The media contents remain unchanged.

1. In the HP OpenView Storage Data Protector Manager, switch to the Devices & Media context. The Scoping Pane displays the list of devices and media configured within your cell when you expand the respective item.
2. Expand the Media item and the media pool, and then select the media you want to export.
3. Right-click one of your selections, click Export, and then confirm your decision.

   The exported media will disappear from the list.

Importing Media

This functionality enables you to reread information about media and their contents back into the IDB. See also "Importing Media" on page 113 for more information.

1. In the HP OpenView Storage Data Protector Manager, switch to the Devices & Media context.
2. Under Devices, expand the device that has the media that you want to import.
3. Expand the Slots item and select the slots that you want to import.
4. In the Actions menu, click Import. The Import wizard appears.
5. Enter the required information, including the media pool that you want to add the media to, the drive that will be associated with the media, as well as any options that you want to set.

The STK ACS Library Device

The concepts, configuration, and installation of the STK ACS library device are basically the same as the steps necessary to use the ADIC/GRAU DAS device with Data Protector. Refer to the "Data Protector and the ADIC/GRAU DAS Library Device" section for additional reference. The ACS Media Agent does not require the preparation necessary for installation of the DAS Media Agent.

Direct Access to the Library: Installation and Configuration

This section focuses on the direct access configuration. The section is structured in the following order:

- Initial steps you have to complete to prepare for installation
- How to install the ACS Media Agent software on Windows and HP-UX platforms
- Using the Data Protector GUI to configure the STK ACS library
- Using the Data Protector GUI to configure drives
- Using the Data Protector GUI to access the STK ACS library

Media Management Basics

Data Protector provides a number of actions available for media in the ACS library, such as querying the library for a complete list of media, and entering or ejecting media from the library. For an overview of the integration, and detailed information on media management, refer to the first section in this chapter, "Data Protector and the ADIC/GRAU DAS and STK ACS Integration."

STK ACS-Specific Media Management

Query puts the volsers (tapes) from all silos controlled by one ACSLS machine into one library. Data Protector needs to use the first value in the CAP entry (for example ACS library1 has CAP 0,0,0 and ACS library2 has CAP 1,0,0) to determine if a tape is in the library that the user is managing. This makes the query function unusable.

Connecting Library Drives

Physically connect the library drives and robotics to the systems where you intend to install the ACS Media Agent software.

See http://www.openview.hp.com/products/datapro/spec_0001.html for details about supported STK libraries.

See "Installing the HP-UX Client System" in the *HP OpenView Storage Data Protector Installation and Licensing Guide* for information on how to physically attach a backup device to a UNIX system.

See "Installing the Windows Client System" in the *HP OpenView Storage Data Protector Installation and Licensing Guide* for information on how to physically attach a backup device to a Windows system.

Installing the ACS Media Agent to Use the StorageTek Library

Data Protector provides a dedicated StorageTek ACS library policy used to configure a Storage Tek ACS library as a Data Protector backup device. You need to install the Data Protector ACS Agent on every system that will be physically connected to a drive in the StorageTek library, even when choosing the indirect library access configuration.

The ACS component includes the standard Data Protector Media Agent functionality, thus the Media Agent must not be installed over existing ACS software.

NOTE

You need special licenses that depend on the number of drives and slots used in the StorageTek library. See "Data Protector Licensing" in the *HP OpenView Storage Data Protector Installation and Licensing Guide* for more information.

Installing the ACS Media Agent on a Windows System

Prerequisites

The following prerequisites for installation have to be met before installing the ACS Agent on a Windows system:

- The StorageTek library has to be configured and running. See the documentation that comes with the StorageTek library.

- Data Protector has to be installed and configured. See *HP OpenView Storage Data Protector Installation and Licensing Guide*.
- The following information has to be obtained before you start installing the ACS Agent software:

  ✓ The *<hostname>* of the host where ACSLS is running.

  ✓ A list of ACS drive IDs that you want to use with Data Protector. To display the list, login on the host where ACSLS is running and execute the following command:

  ```
  rlogin "ACSLS hostname" -l acssa
  ```

  ✓ You will have to enter the terminal type and wait for the command prompt. At the ACSSA prompt, enter the following command:

  ```
  ACSSA> query drive all
  ```

  The format specification of an ACS drive has to be the following:

  ```
  ACS DRIVE: ID:#,#,#,# - (ACS num, LSM num, PANEL,
  DRIVE).
  ```

  ✓ Make sure that the drives that will be used for Data Protector are in the state `online`. If a drive is not in the `online` state, change the state with the following command on ACSLS host:

  ```
  vary drive <drive_id> online
  ```

  ✓ A list of available ACS CAP IDs and ACS CAP format specification. To display the list, login on the host where ACSLS is running and execute the following command:

  ```
  rlogin "ACSLS hostname" -l acssa
  ```

  You will have to enter the terminal type and wait for the command prompt. At the ACSSA prompt, enter the following command:

  ```
  ACSSA> query cap all
  ```

  The format specification of an ACS CAP has to be the following:

  ```
  ACS CAP: ID:#,#,# (ACS num, LSM num, PANEL, DRIVE).
  ```

  ✓ Make sure that the CAPs that will be used for Data Protector are in the state `online` and in `manual` operating mode.

  If a CAP is not in the state `online`, change the state using the following command:

  ```
  vary cap <cap_id> online
  ```

If a CAP is not in `manual` operating mode, change the mode using the following command:

```
set cap manual <cap_id>
```

✓ A list of SCSI addresses for the drives, for example, scsi4:0:1:0.

For more information on SCSI addresses, see *HP OpenView Storage Data Protector Installation and Licensing Guide*.

Remote Installation

The installation procedure consists of the steps:

1. Distribute the ACS Agent component to clients using the Data Protector graphical user interface and Installation Server for Windows.
2. Physically connect the library drives and the systems where you have installed ACS Agent.

   See http://www.hp.com/go/dataprotector/specification for details about supported StorageTek devices.
3. To start the ACS `ssi` daemon
   - On the Windows ACS client and the Cell Manager, install the `LibAttach` service. Make sure that during configuration of `LibAttach` service the appropriate ACSLS hostname is entered. After the successful configuration the `LibAttach` services are started automatically and will be started automatically after the boot as well.

NOTE

After you have attached the `LibAttach` service, check if the `libattach\bin` directory has been added to the system path automatically. If not, add it manually.

   - For more information on the service see the documentation that comes with the StorageTek library.
4. Run the following command to check whether or not the library drives are properly connected to your system:
   - On Windows ACS client,

     `<Data_Protector_home>\bin\devbra -dev`

You should see the library drives with corresponding device files/SCSI addresses displayed in the list.

Installing the ACS Media Agent on a 32-bit HP-UX System

Prerequisites

The following prerequisites for installation have to be met before installing the ACS Agent on an HP-UX system:

- The StorageTek library has to be configured and running. See the documentation that comes with the StorageTek library.
- Data Protector has to be installed and configured. See the *HP OpenView Storage Data Protector Installation and Licensing Guide*.
- The following information has to be obtained before you start installing the ACS Agent software:
  - ✓ The *<hostname>* of the host where ACSLS is running.
  - ✓ A list of ACS drive IDs that you want to use with Data Protector. To display the list, login on the host where ACSLS is running and execute the following command:

    ```
    rlogin "ACSLS hostname" -l acssa
    ```

  - ✓ You will have to enter the terminal type and wait for the command prompt. At the ACSSA prompt, enter the following command:

    ```
    ACSSA> query drive all
    ```

    The format specification of an ACS drive has to be the following:

    ```
    ACS DRIVE: ID:#,#,#,# - (ACS num, LSM num, PANEL,
    DRIVE).
    ```

  - ✓ Make sure that the drives that will be used for Data Protector are in the state `online`. If a drive is not in the `online` state, change the state with the following command on ACSLS host:

    ```
    vary drive <drive_id> online
    ```

  - ✓ A list of available ACS CAP IDs and ACS CAP format specification. To display the list, login on the host where ACSLS is running and execute the following command:

    ```
    rlogin "ACSLS hostname" -l acssa
    ```

    You will have to enter the terminal type and wait for the command prompt. At the ACSSA prompt, enter the following command:

```
ACSSA> query cap all
```

The format specification of an ACS CAP has to be the following:

```
ACS CAP: ID:#,#,#,# - (ACS num, LSM num, PANEL,
DRIVE).
```

✓ Make sure that the CAPs that will be used for Data Protector are in the state `online` and in `manual` operating mode.

If a CAP is not in the state `online`, change the state using the following command:

```
vary cap <cap_id> online
```

If a CAP is not in `manual` operating mode, change the mode using the following command:

```
set cap manual <cap_id>
```

✓ A list of UNIX device files for the drives.

Run the `ioscan -fn` system command on your system to display the required information.

For more information on UNIX device files, see *HP OpenView Storage Data Protector Installation and Licensing Guide*

Remote Installation

The installation procedure consists of the steps:

1. Distribute the ACS Agent component to clients using the Data Protector graphical user interface and Installation Server for UNIX. See the *HP OpenView Storage Data Protector Installation and Licensing Guide*.
2. Physically connect the library drives and the systems where you have installed ACS Agent.

   See http://www.openview.hp.com/products/datapro/spec_0001.html for details about supported StorageTek devices.

   See the *HP OpenView Storage Data Protector Installation and Licensing Guide* for information about how to physically attach a backup device to the system. Also see the documentation that comes with the StorageTek library.
3. To start the ACS `ssi` daemon
   - on UNIX ACS client, run the following command:

```
/<Data_Protector_home>/acs/ssi/ssi.sh start
<ACS_LS_hostname>
```

4. On UNIX ACS client, run the following command to check whether or not the library drives are properly connected to your system:

   ```
   /opt/omni/lbin/devbra -dev
   ```

   You should see the library drives with corresponding device files/SCSI addresses displayed in the list.

Using Data Protector to Configure the STK ACS Library

The direct library access configuration is the same as the ADIC/GRAU DAS library direct access configuration. Follow the GUI steps provided in the section "Using Data Protector to Configure the ADIC/GRAU Library and Drives" on page 671. Instead of choosing `GRAU DAS Library` as your device type, choose `Storage Tek ACS Library`.

Using Data Protector to Configure Drives

To configure drives in the STK ACS library, follow the same steps provided in the ADIC/GRAU DAS section "Using Data Protector to Configure Drives" on page 670.

Indirect Access to the Library: Installation and Configuration

This section focuses on the indirect access configuration.

Using Data Protector to Configure the STK ACS Library and Drives

The indirect access configuration steps are the same as the direct access configuration (see previous section for steps), except the default setting, `Force Direct Library Access`, should be turned off.

- Follow the same GUI steps as for the direct library access configuration. When the library configuration is complete, you will be prompted to create library drives.

- Follow the same steps for creating drives as in the indirect library access configuration, but in Advanced Options, make sure to turn off the Force Direct Library Access feature. By default, this feature is on.

Using Data Protector to Access the STK ACS Library

Once you have configured your environment and installed the ACS Media Agent on the systems that will access the library robotics, you are ready to use the Data Protector GUI to access the media in the STK ACS library. The following sections provide instructions on using Data Protector with the STK integration.

NOTE

Data Protector allows you to connect directly to the ACS Library Server host and perform some management tasks.

To connect to the ACS Library Server host, choose Actions, Connect to ACSLM from the Library Management window.

This action performs a remsh command to the ACSLS host and starts cmd_proc. If you want to change the default settings for this action, change the ACSLMHOST option in the global options file.

Searching for Media

Use this function to locate a specific medium without having to browse the entire list of media. Data Protector locates media by searching through Medium Labels, then Medium Locations, and finally Medium IDs.

1. In the HP OpenView Storage Data Protector Manager, switch to the Devices & Media context.
2. To search for media in a media pool, select the Media item.

   To search for media in a library, select the Devices item.
3. In the Edit menu, click Find. The Find dialog box appears.

   Use the appropriate search method to search for media.

Entering Media

Use this functionality to physically enter media into an STK repository and automatically register added media as members of the library.

1. In the HP OpenView Storage Data Protector Manager, switch to the Devices & Media context.
2. In the Scoping Pane, click Devices. The list of configured devices will display in the Results Area.
3. In the list of configured devices click the name of the library, then expand it to display the Drives and Slots items.
4. Click Slots to display the list of media in the Results Area.
5. Select the media that you want to enter.
6. In the Actions menu, click Enter to eject the media to the I/O Cap.

   See online Help for further information.

Ejecting Media

Use this functionality to physically move selected media from the repository into the CAP area.

1. In the HP OpenView Storage Data Protector Manager, switch to the Devices & Media context.
2. In the Scoping Pane, click Devices. The list of configured devices will display in the Results Area.
3. In the list of configured devices click the name of the library, then expand it to display the Drives and Slots items.
4. Click Slots to display the list of media in the Results Area.
5. Select the media you want to eject.
6. In the Actions menu, click Eject Medium to eject the medium to the I/O Cap.
7. Open the CAP, remove the media, and close the Cap.

   See online Help for further information.

Adding Media to a Media Pool

Adding media to a media pool registers the new media in the IDB as members of this media pool. It is not necessary for these media to actually reside in the ACS repository.

To add media to a pool, initialize it first. Initializing media prepares it for use with Data Protector. See "Initializing Media." You can also import it. See "Importing Media."

Initializing Media

Initializing media prepares media for use with Data Protector by saving the information about the media (medium ID, description and location) in the IDB and also writes this information on the medium itself (media header). When you initialize media, you also specify to which media pool the media belongs.

You need to initialize media before you use media for backup. If media are not initialized before backup, Data Protector formats media during backup. This increases the backup time.

Initializing Individual Media

1. In the HP OpenView Storage Data Protector Manager, switch to the Devices & Media context.
2. Expand the Media item, right-click the desired media pool, and then select Initialize. The Initialize wizard appears.
3. In the Destination page, in the Media Pool drop-down box, select the media pool to which the media will be assigned. Click Next.
4. In the Medium Location drop-down list, select which device the media are in.
5. Click Next. The Medium Name page appears.
6. Under Medium Name, either have Data Protector Automatically Generate a name for the medium, or click the Specify radio button and enter a name for the medium in the accompanying text box.
7. In the informational User Location drop-down box, either enter or select the location of the media's user.
8. Click Next. The Initializing Options page appears.

The Medium Capacity button defines whether Data Protector will Determine the storage size of the medium, or whether you want to Specify the storage size of the medium. You can leave the default, which is Determine.

The Force Initialization button will automatically initialize blank media or media in other formats recognized by Data Protector (tar, cpio, OmniBackI, and so on). You can leave the default value. Data Protector media containing protected data will not be re-initialized even if this option is set. The Eject option, if set, will eject a medium from the drive after the initialization completes.

Follow online Help for information on specific items in the wizard.

9. Click Finish to confirm and exit this wizard.

Initializing Multiple Media in a Library Device

1. In the HP OpenView Storage Data Protector Manager, switch to the Devices & Media context.
2. Under Devices, expand the library device that contains the media that you want to initialize.
3. Expand the Slots item, and then select a range of slots to initialize.

   Right-click the selected range of slots, and then select Initialize. The Initialize wizard appears.
4. In the Destination page, in the Media Pool drop-down box, select the media pool to which the media will be assigned.
5. Click Next.The location page appears.
6. In the Medium Location drop-down list, select which device the media are in.
7. Click Next. The Medium Name page appears.
8. Under Medium Name, either have Data Protector Automatically Generate a name for the medium, or click the Specify radio button and enter a name for the medium in the accompanying text box.
9. In the informational User Location drop-down box, either enter or select the location of the media's user.
10. Click Next. The Initializing Options page appears.

11. Optionally, use the Medium Capacity button to define whether Data Protector will Determine the storage size of the medium, or whether you want to Specify the storage size of the medium. You can leave the default, which is Determine.
12. Optionally, using the Force Initialization button will automatically initialize blank media or media in other formats recognized by Data Protector (tar, cpio, OmniBackI, and so on). You can leave the default value. Data Protector media containing protected data will not be re-initialized even if this option is set. The Eject option, if set, will eject a medium from the drive after the initialization completes.

    Follow online Help for information on specific items in the wizard.
13. Click Finish to confirm and exit this wizard.

Verifying Media

Use this function to verify media in a media pool. By reading all media blocks and parsing all the headers, then parsing all Media Agent blocks and checking records in each block, Data Protector determines whether the data on the media is valid. If the CRC option was set during backup, Data Protector recalculates the CRC and compares the values.

You can only verify resident Data Protector media.

1. In the HP OpenView Storage Data Protector Manager, switch to the Devices & Media context.
2. In the Scoping Pane, click Devices. The list of configured devices will display in the Results Area.
3. In the list of configured devices click the name of the library, then expand it to display the Drives and Slots items.
4. Click Slots to display the list of slots in the Results Area.
5. Select a range of media to verify.
6. Right-click your selected media, and then click Verify.

   See online Help for further information.

Scanning Media

Use this function to examine the format of selected media. Also see "Scanning Media in a Device" on page 129 for more information.

1. In the HP OpenView Storage Data Protector Manager, switch to the Devices & Media context.
2. In the Scoping Pane, click Devices. The list of configured devices will display in the Results Area.
3. In the list of configured devices click the name of the library, then expand it to display the Drives and Slots items.
4. Click Slots to display the list of volsers in the Results Area.
5. Select a range of media to scan.
6. Right-click your selected media, and then click Scan.

   See online Help for further information.

When the scan process has been completed, the Library Management window is updated with information on the format of the examined media.

Modifying Media Attributes

Use this function to change the location or label description of a Data Protector medium. An example of when you might want to change the location of a medium could be when the medium is sent to offsite storage.

1. In the HP OpenView Storage Data Protector Manager, switch to the Devices & Media context.
2. In the Scoping Pane, click Devices. The list of configured devices will display in the Results Area.
3. In the list of configured devices click the name of the library, then expand it to display the Drives and Slots items.
4. Click Slots to display the list of media in the Results Area.
5. Select a medium to modify.
6. Change the information that appears in the Results Area.

   See online Help for further information.

NOTE These modifications are made to the IDB, and not to the tape itself.

Moving Media

Use this function to move media from one media pool to another. When you move media to another media pool, all the media information such as condition, type, medium ID, and session information is transferred to the new media pool.

Getting Information about Media

Use this functionality to display detailed information about the usage and condition of an individual selected Data Protector medium. *This is a read-only window.*

1. In the `HP OpenView Storage Data Protector Manager`, switch to the `Devices & Media` context.
2. In the Scoping Pane, click `Devices`. The list of configured devices will display in the Results area.
3. In the list of configured devices click the name of the library, then expand it to display the `Drives` and `Slots` items.
4. Click `Slots` to display the list of slots in the Results Area.
5. Select a medium to view.
6. Information about the medium appears in the Results Area.

   See online Help for further information.

Querying the STK ACSLM Host

If you want to get information about a repository in the STK library from the server, you can query the ACSLM host. Querying ACSLM queries the ACSLS database, and then synchronizes the information in the IDB with what is actually in the repository.

This is especially useful if you were using STK commands to manage media, as this results in inconsistencies with the IDB - Data Protector does not know the latest status of media in the library repository.

1. In the `HP OpenView Storage Data Protector Manager`, switch to the `Devices & Media` context.
2. In the list of configured devices click the name of the library, then expand it to display the `Drives` and `Slots` items.
3. Right-click the device that you want to query, and then click `Query`.

See online Help for further information.

This action queries the ASCLM host for information.

Recycling Media

Recycling a Data Protector owned media removes protection from data objects contained on the media. A recycled medium can be reused for backup. Also see "Recycling Media" on page 123 for more information.

1. In the HP OpenView Storage Data Protector Manager, switch to the Devices & Media context.
2. In the Scoping Pane, click Devices. The list of configured devices will display in the Results Area.
3. In the list of configured devices click the name of the library, then expand it to display the Drives and Slots items.
4. Select and then right-click the media that you want to recycle.
5. Click Recycle.

   See online Help for further information.

Removing Media

This action does not affect media in the STK library but only removes specific media from IDB. Therefore, Data Protector does not know that these media exist and does not use them.

1. In the HP OpenView Storage Data Protector Manager, switch to the Devices & Media context.
2. Under Devices, expand the device that has the media that you want to export.
3. Expand the Slots item and select the media that you want to export.
4. In the Actions menu, click Export. The confirmation dialog box appears for you to confirm that you want to export the selected media.
5. Click OK to export the selected media.

NOTE If the number of media to be removed at once exceeds fourteen, the media will not be referred to by ID (displayed in the window). You will be asked if you wish to remove that amount of media.

Exporting Media

This functionality enables you to remove information about backup objects contained on a Data Protector medium from the IDB. Use it when media will no longer be used in a Data Protector cell. The media contents remain unchanged.

1. In the `HP OpenView Storage Data Protector Manager`, switch to the `Devices & Media` context. The `Scoping Pane` displays the list of devices and media configured within your cell when you expand the respective item.
2. Expand the `Media` item and the media pool, and then select the media you want to export.
3. Right-click one of your selections, click `Export`, and then confirm your decision.

   The exported media will disappear from the list.

Importing Media

This functionality enables you to reread information about media and their contents back into an IDB. See also "Importing Media" on page 113 for more information.

1. In the `HP OpenView Storage Data Protector Manager`, switch to the `Devices & Media` context.
2. Under `Devices`, expand the device that has the media that you want to import.
3. Expand the `Slots` item and select the media that you want to import.
4. In the `Actions` menu, click `Import`. The `Import` wizard appears.
5. Enter the required information, including the media pool that you want to add the media to, the drive that will be associated with at media, as well as any options that you want to set.

   See online Help for a description of the fields and options.

Observe messages generated during the process in the Library Management window.

Troubleshooting Library Installation and Configuration

Installation Steps

1. Install the DAS Media Agent on the system controlling the GRAU robotics (PC/robot).
2. Install the DAS Media Agent on the NT PCs where a drive is connected (PC/drive).
3. Copy `aci.dll + winrpc.dll + ezrpcw32.dll` to `winnt\system32` and *<Data_Protector_home>*`\bin` directory.
4. Create `aci` directory on PC/robot.
5. Copy `dasadmin.exe` to this directory.
6. Copy `portmapper` and `portinst` to `aci` directory.
7. Start `portinst` to install `portmapper` (only on PC/robot).
8. Install `mmd` patch on the CM.
9. The PC needs to be rebooted; then open Windows `Control Panel`. Go to `Services` (Windows NT) or `Administrative Tools, Services` (other Windows systems) and check if `portmapper` and both rpc services are running.
10. Go to the OS/2 PC within the GRAU library, edit the `/das/etc/config` file:

    `cd /das/etc/`

    execute: `"e config"`

    Within this config file you need to add a client called DATA_PROTECTOR containing the IP address of the PC/robot.
11. Execute the following commands from PC/robot:

    `dasadmin listd`

    `dasadmin` all DLT7000 UP *<AMUCLIENT>*

    `dasadmin mount` *<VOLSER>* (then you need to push the `UNLOAD` button on the drive)

    `dasadmin dismount` *<VOLSER>*

(or: `dasadmin dismount -d <DRIVENAME>`)

where *<AMUCLIENT>* = DATA_PROTECTOR

and *<VOLSER>* for example = 001565

and *<DRIVENAME>* is for example = DLT7001

and "all" stands for "allocate"

If you are not successful with these commands (communication to DAS Server (OS/2), try to execute these commands on the OS/2 PC. You can find the `dasadmin` command in `/das/bin/`.

If you execute theses commands from the OS/2 PC, use *<AMUCLIENT>* = `AMUCLIENT`.

1. Login to the AMU client. The common login are the following:

   `user: Administrator pwd: administrator`

   `user: Supervisor pwd: supervisor`

2. It may be necessary to set the media type:

   set `ACI_MEDIA_TYPE` set `ACI_MEDIA_TYPE=DECDLT`

3. To reboot the library, proceed as follows:

   Shutdown OS/2 and then switch off robotics.

   Restart OS/2 and when OS/2 is ready, the AMU log will display that the robotics is not ready. Then, switch on robotics.

How to Configure GRAU CAPs?

You can only move media from the CAP to a slot and then to a drive, using the device's robotics. You have to use `import` and `export` commands. For example:

```
import CAP: I01
import CAP range: I01-I03
export CAP: E01
export CAP range: E01-E03
```

How to Use uma Utility?

The following syntax is used when you use the Data Protector `uma` utility to manage the GRAU and STK library drives:

```
uma -pol 8 -ioctl grauamu
pol 8 for GRAU
```

```
pol 9 for STK
```

The default media type is DLT.

COBRA TECNOLOGIA
Integradora de Soluções em TI e Serviços

24365 Paula

ANEXO UNIDADE DE BACKUP ROBOTIZADO
PARTE D/9

COBRA Tecnologia S.A.
Estrada dos Bandeirantes 7966
CEP 22783-110 Rio de Janeiro RJ
Tel. 21 2442-8800
www.cobra.com.br

A Further Information

In This Appendix

This chapter gives information on the following topics:

Backing Up and Restoring UNIX Specifics

This section explains how to backup specific UNIX formats, including VxFS, Enterprise Filesystems, and Context Dependent Filesystems.

VxFS Snapshot

What Is VxFS?

VxFS allows you to back up a filesystem while it is being used by some other application. This is called an online backup and is done by creating a snapshot of a filesystem and backing up this snapshot.

You create a snapshot of a filesystem when you mount the VxFS filesystem to a temporary directory. At this point you also specify the filesystem you want to snap.

A **snapshot** is a copy of the filesystem at a specific moment in time you mount the VxFS filesystem to a temporary directory.

You can perform normal backups without using the VxFS snapshot feature by simply configuring a backup as for any other filesystem. In this case you cannot back up files that are in use.

You configure a backup of this temporary directory, which is actually a mountpoint to the snapshot of the filesystem as it was at the moment of the mount.

When the backup is finished, you unmount the snapshot filesystem so that it can be used for other purposes.

How to Configure VxFS Backup?

If you want to use the VxFS online backup functionality, you must configure the backup as follows:

1. You have to have an empty or unused partition created on your system that can be used by VxFS for a snapshot. See your system administrator's manual for instructions.

   The recommended size for the snapshot filesystem is up to 15% of the snapped filesystem, if the filesystem is used heavily use during the backup. Normally, the size should be around 5%.

If the amount of data modified on the snapped filesystem is higher than the space available, Data Protector produces `Cannot stat` error messages for all the remaining files to be backed up. You must unmount the snapshot filesystem and repeat the backup procedure.

2. Create a temporary directory to which you will mount the snapshot filesystem.
3. Create shell scripts to mount and unmount the snapshot filesystem to the temporary directory. See "Pre- and Post -exec Script Templates" in the next section for templates of these scripts.
4. Configure a backup of the temporary directory. The mount script must be specified as the Pre- exec command, and the unmount script as the Post-exec command.

Pre- and Post- exec Script Templates

Here are example templates that can be configured as Data Protector Pre- exec and Post- exec commands to mount or unmount the VxFS filesystem.

Example A-1 **Pre- exec Script Template**

```
# SnapMount.sh
#
# Mounting snapshot filesystem (Pre-exec script)
#
# A script requires 3 parameters:
# 1. a block special file of the snapped FS
# or
# a mount point directory of the snapped FS
# 2. a block special file of the snapshot FS
# 3. a mount point of the snapshot FS
#
# NOTE:
#
# In case of multiple Disk Agents reading from the same
snapshot
# FS,
# the Pre-exec script should contain a kind of
synchronization
# mechanism for following reasons:
#
# 1) an attempt to mount an already mounted snapshot FS,
```

```
# snapping the same FS will cause the Pre-exec script to
fail and
# a DA to abort
#
# 2) an attempt to mount an already mounted snapshot FS,
# snapping some other FS will cause a warning to be
generated,
# script to fail and a DA to abort
#
# 3) a synchronization with the Post-exec script should
be also
# provided because the snapshot FS must not be unmounted
while
# there is other DA reading from the FS.
#


SNAPPED_FS=$1
SNAPSHOT_FS=$2
MOUNT_POINT=$3


mount -F vxfs -e -o snapof=$SNAPPED_FS $SNAPSHOT_FS
$MOUNT_POINT


#
# end SnapMount.sh
#
```

The template below can be used to unmount a VxFS system.

Example A-2 **Post- exec Script Template**

```
# SnapUnmount.sh
#
# Unmounting snapshot filesystem (Post-exec shell
script)
#
# Script requires 1 parameter:
# - a mount point directory of the snapshot FS
# or
```

```
# - a block special file of the snapshot FS
#
# NOTE
# In case of multiple Disk Agents reading from the same
snapshot
# FS, a kind of synchronization mechanism has to be added
for
# the following reasons:
#
# 1) Post-exec script should unmount snapshot FS only if
there
# is no other DA reading from the snapshot FS
#
# Success/failure of the DA can be checked by examining
# the BDACC environment variable
#

MOUNT_POINT=$1

umount -v $MOUNT_POINT


#
# end SnapUnmount.sh
#
```

Data Protector Commands

For a complete list of supported Data Protector commands, refer to the *HP OpenView Storage Data Protector Command Line Interface Reference* (`CLIReference.pdf`) or the `omniintro` man page on UNIX.

The *HP OpenView Storage Data Protector Command Line Interface Reference* is located in the *<Data_Protector_home>*`\docs\MAN` directory on Windows or in the `/opt/omni/doc/C/` directory on UNIX.

The documents are available, if you installed the `User Interface` component on Windows or the `OB2-DOCS` component on UNIX.

On UNIX, use `man` *<command_name>* for more details about the command.

Performance Considerations

This section gives an overview of the most common backup performance factors. It is not meant to discuss performance. Due to the high number of variables and permutations, it is not possible to give distinct recommendations that fit all user requirements and affordable investment levels. Further discussions can be found in the *HP OpenView Storage Data Protector Concepts Guide*.

The Infrastructure

The infrastructure has a high impact on backup and restore performance. The most important factors are the parallelism of data paths and the use of high speed equipment.

Network Versus Local Backups and Restores

Sending data over the network introduces additional overhead, as the network becomes a component to performance consideration. Data Protector handles the datastream differently for the following cases:

Network Datastream Disk to Memory to Network to Memory to Device

Local Datastream Disk to Memory to Device

In order to maximize the performance, it is recommended to use local backup configurations for high volume datastreams.

Devices

The device type and model impacts the performance because of the sustained speed at which a device can write data to a tape (or read data from it). For example:

- DDS/DAT devices typically have a sustained speed of 510 KB/s to 3 MB/s, without compression, depending on the model.
- DLT devices typically have a sustained speed of 1.5 MB/s to 6 MB/s, without compression, depending on the model.
- LTO devices typically have a sustained speed of 10 MB/s to 20MB/s, without compression, depending on the model.

The speed also varies if a device-compression gets used. The achievable compression ratio depends on the nature of the data being backed up. For most cases, using high speed devices with device-compression ON does improve performance. This however is true only if the device(s) stream.

Libraries offer additional advantages because of their fast and automated access to a large number of media. At a backup time loading new or reusable media is needed and at a restore time the media which contain the data to be restored need to be accessed quickly.

High Performance Hardware Other Than Devices

The computer systems themselves, that is, reading the disk and writing to the device, directly impact performance. The systems are loaded during backup by reading the disk or handling software (de-)compression.

The disk read data rate and available CPU are important performance criteria for the systems themselves in addition to the I/O performance and network types.

Using Hardware in Parallel

Using several datapaths in parallel is a fundamental and efficient method to improve performance. This includes the network infrastructure. Parallelism helps in the following situations:

- Several systems can be backed up locally, that is, with the disk(s) and the related devices connected on the same system.
- Several systems can be backed up over the network. Here the network traffic routing needs to be such that the datapaths do not overlap, otherwise the performance will be reduced.
- Several objects (disks) can be backed up to one or several (tape) devices.
- Several dedicated network links between certain systems can be used. For example, system_A has 6 objects (disks) to be backed up, and system_B has 3 fast tape devices. Putting 3 network links dedicated to backup between system_A and system_B is a solution.

- Load Balancing: This is where Data Protector dynamically determines which filesystem should be backed up to which device. Normally, it is best to enable this feature. This is especially true when a large number of filesystems in a dynamic environment are being backed up.

Configuring Backups and Restores

Any given infrastructure must be used efficiently in order to maximize performance. Data Protector offers high flexibility in order to adapt to the environment.

Device Streaming

To maximize a device's performance, it must be kept streaming. A device is streaming if it can feed enough data to the medium to keep it moving forward continuously. Otherwise, the tape has to be stopped, the device waits for some more data, reverses the tape a little and resumes to write to the tape, and so on. In other words, if the data rate written to the tape is less or equal the data rate which can be delivered to the device by the computer system, then the device is streaming. In network-focused backup infrastructures, this deserves attention.

Backups can be setup so that the data from several disk agents is sent to one Media Agent, which sends the data to the device.

Block Size

The device hardware processes data it receives using a device type specific block size. Data Protector allows to adjust the size of the block it sends to the device. The default value is 64kB.

Increasing the block size can improve the performance. Changing the block size should be done *before* formatting tapes. For example, a tape written with the default block size cannot be appended to a tape using a different block size.

Software Compression

Software compression is done by the client CPU when reading the data from the disk. This reduces the data which gets send over the network, but it requires significant CPU resources from the client.

NOTE By default, software compression should be disabled. Software compression should only be used for backup of many systems over a slow network where the data can be compressed before sending it over the network. If software compression is used, hardware compression should be disabled since trying to compress data twice actually expands the data.

Hardware Compression

Hardware compression is done by a device, which receives the original data from the Media Agent client and writes it to the tape in compressed mode. Hardware compression increases the speed at which a tape drive can receive data, because less data is written to the tape.

By default, hardware compression should be enabled. On HP-UX and Solaris, hardware compression should be enabled by selecting a hardware compression device file. On Windows NT and Windows 2000, hardware compression can be selected during the device configuration. Using hardware compression or not should be a conscious decision, because media written in compressed mode cannot be read using the device in uncompressed mode and vice-versa.

Limitations HP Ultrium LTO drives use automatic hardware compression which cannot be disabled. Ensure that you do not enable `Software compression` when you configure an HP Ultrium LTO drive.

Full and Incremental Backups

A basic approach to improve performance is to reduce the amount of backed-up data. Take full advantage of time and resources when planning your full and incremental backups. An important consideration is that there is no need to do full backups of all the systems on the same day, unless necessary. See the *HP OpenView Storage Data Protector Concepts Guide* for more information.

Image Backup Versus Filesystem

It used to be more efficient to back up images (raw volumes) instead of backing up filesystems. This can still be true in some cases, such as with heavily-loaded systems or if the disks contain a large number of scattered files. The general recommendation is to use the filesystem backup.

Object Distribution to Media

There are many ways to configure a backup such that the backup data ends up on the media in just as many different configurations. For example:

- One object goes to one medium, or
- Several objects go to several media, each medium contains data from each object

Under certain conditions, one distribution may be advantageous considering the backup performance, however this may not be the optimal restore configuration.

The challenge is to optimize the setup for a backup (since it is done frequently) and at the same time have an acceptable restore media situation.

Miscellaneous Performance Hints

- Patches:

  Ensure you have installed all patches pertaining the performance on the network.

- On the computers that are Media Agent and Disk Agent clients, set the IP as shown below:

  ```
  IP is local "<MA_And_DA_Client_name>" == true
  ```

- LAN Cards:

  If you use a FDDI card, you can move it up on the bus so that it receives a higher priority. Use `ftp` to transfer large files between the MA and DA systems to see how the speed compares to Data Protector performance. The network cards configured in half-duplex decrease the performance.

- Simulating a high-speed device:

If you suspect that the sustained data flow to the tape device is too low or that the device does not handle it correctly, you can simulate a very fast device on the Media Agent client by doing the following:

1. Create a standalone file device and a device file `/dev/null` on UNIX and `nul` on Windows.
2. Create a separate pool and select `loose` policy.
3. Set `InitOnLoosePolicy=1` and set data protection to `None`. Perform backups to this device and check if the performance discrepancy between backups to the file device and backups to the real device can be explained.You can also run the `vbda` locally and write directly to a file. Run the commands listed below:

   On HP-UX and Solaris:

   ```
   /opt/omni/lbin/vbda -vol /home -trees /home/jdo -
   out /dev/null -profile
   ```

   On Windows:

   ```
   <Data_Protector_home>\bin\vbda -vol /C -trees
   "/Program Files/OmniBack/bin" -out nul -profile
   ```

   On Novell NetWare:

   ```
   load sys:usr\omni\bin\hpvbda.nlm -vol /sys -tree
   /usr/omni -out \tmp\test
   ```

- Device configuration

  Adjust the device block size if necessary.

- CRC option

  CRC option impacts performance due to the CRC calculation, which is performed by the Media Agent client.

- Logging and Report Level

  If an update of the IDB takes too long, disable logging by setting it to `Log None`. The same way you can filter messages by setting the Report level to `Critical`.

- Data Protector Application Clients

  If a restore session of the Application clients (Oracle, SAP R/3) takes too long, decrease the SmWaitforNewClient value, which is by default 5 minutes. Set it to a lower value.

Example of Scheduled Eject of Media

You might want to eject all media that were used for backup during the night every morning at 6.00 AM. To schedule such an operation proceed as follows:

Schedule the Report Group

1. In the Data Protector GUI, select `Reporting`.
2. In the Scoping Pane expand `Reporting` and right click `Reports`. Select `Add Report Group`. The `Add Report Group` wizard is displayed.
3. In the wizard, name your report group and click `Next`. The Data Protector Scheduler is displayed.
4. In the Scheduler, select the starting day and click `Add`. In the `Schedule Report Distribution` dialog window, specify the hour, and that the report is to be generated daily. Click `OK` and then `Finish`.

   The Report Group is now scheduled. Now you can add the report to it.

Add the Report to the Report Group and Configure It

1. In the `Add New Report Wizard`, select `Reports on Media and Pools`.
2. Select the `List of Media` type and name the report. Click `Next`.
3. To eject *all* media, regardless of media pool and location leave all fields set to default settings. Click `Next` four times.
4. Select the `Relative time` and specify `8` for `Started within last hours` and `8` for `Duration hours` text boxes respectively. This will cause only the media that were used for backup in the last eight hours from the point of starting a report to be listed in the report. Click `Next`.
5. In the `Format` and `Send` text boxes, select `Tab` and `External`, respectively. In the `Script` text box, provide the name of the script (HP-UX and Solaris systems) or the batch file containing the command that starts the script (Windows systems). The script is

given in the next section. The script (HP-UX and Solaris systems) or the starting batch file (Windows systems) must reside in the `/opt/omni/lbin` (HP-UX and Solaris systems) or *<Data_Protector_home>*\bin (Windows systems) directory.

On Windows systems, the contents of the batch file containing command for starting the script is:

<perl_home>\perl.exe
"*<Data_Protector_home>*\bin\omnirpt_eject.pl"

6. Click the >> button to add this recipient. Click `Finish`.

The Report Group is now scheduled and configured.

Copy the Script to the Specified Directory

Copy or create the script with the name `omnirpt_eject.pl` in the `/opt/omni/lbin` (HP-UX and Solaris systems) or *<Data_Protector_home>*\bin directory (Windows systems).

```
#!/usr/contrib/bin/perl

#=========================================================
========================

#   FUNCTION    Library_Eject

#

#   ARGUMENTS   param 1 = Library to eject from

#               param 2 = Slots to eject

#

#   DESCRIPTION Function ejects specified slots from
specified library

#=========================================================
========================

sub Library_Eject {

    local ($lib,$slots)=@_;

    print "[Normal] Ejecting slot(s) ${slots}from
library \"$lib\"\n";

    print("[Normal] Executing \"${OMNIBIN}omnimm\"
-eject \"$lib\" $slots\n");
```

```
    $report =`"${OMNIBIN}omnimm" -eject \"$lib\"
$slots`;
    #print "\debug>\n$report\n<debug\n";
    if ($report !~/Final report: (\d+) cartridges out of
(\d+) successfully ejected\./) {
        print "[Critical] Eject has
failed!\n\nReport:\n$report\n";
        return (1);
    }
    print "$report\n";
    if ($1 ne $2) {
        print "[Warning] Not all media successfully
ejected!\n";
        return (2);
    }
    print "[Normal] Eject from library \"$lib\"
successfully completed.\n";
    return (0);
}
#============================================================
=========================
#   FUNCTION    Eject
#
#   ARGUMENTS   none
#
#   DESCRIPTION Function for each library in %List call
Library_Eject
#============================================================
=========================
sub Eject {
    local ($lib,$slot,$result);
```

```
    while (($lib, $slot) = each(%List)) {
        $result |=&Library_Eject($lib,$slot);
    }
    if ($result) {
        return (1);
    } else {
        print "[Normal] All operations successfully
completed.\n";
        return (0);
    }
}
#============================================================
=========================
#   FUNCTION    Omnirpt
#
#   ARGUMENTS   none
#
#   DESCRIPTION Function get slots to eject from omnirpt
report
#============================================================
=========================
sub Omnirpt {
    @lines =<STDIN>;
    for ($i=5;$i<@lines;$i++) {
        @line =split(/\t/,$lines[$i]);
        if ($line[2] =~/^\[([\w:\-\s]+):\s+(\w+)\]/) {
           $List{$1}.=$2.' ';  # $1= "Library name", $2=
"Slot ID"
        }
    }
```

```
    if (!keys(%List)) {
        print "[Warning] No tape(s) to eject.\n";
        return (1);
    }
    return (0);

}
#-----------------------------------------------------------
-----------------
#                                    MAIN
#-----------------------------------------------------------
-----------------
if ($ENV{"OS"}=~/Windows/) {  # Windows NT
      $OMNIBIN ='c:\\program files\\omniback\\bin\\';
    } else {
        local($uname)=`uname -a`;
        chop $uname;
        @uname=split(' ', $uname);
        if ($uname[0]) {
            if ($uname [0] eq 'HP-UX') {
                $OMNIBIN ='/opt/omni/bin/';
            } else {
                $OMNIBIN ='/usr/omni/bin';
            }
        } else {
            exit (1);
        }
    }
```

```
    print "[Normal] Starting eject of media that have
been used in the last 24 hours.\n";

    exit (0) if (&Omnirpt());
    exit (1) if (&Eject());
```

Examples of Pre-Exec and Post-Exec Commands for UNIX

The following scripts are some examples of Pre- and Post- exec commands on UNIX.

Session Pre-Exec: Shut Down Application

The script shuts down an Oracle instance.

```
#!/bin/sh
export ORACLE_HOME=$2
export ORACLE_SQLNET_NAME=$1
if [ -f $ORACLE_HOME/bin/svrmgrl ]; then
$ORACLE_HOME/bin/svrmgrl << EOF
connect sys/manager@$ORACLE_SQLNET_NAME as sysdba
shutdown
EOF
echo "Oracle database \"$ORACLE_SID\" shut down."
exit 0
else
echo "Cannot find Oracle SVRMGRL
($ORACLE_HOME/bin/svrmgrl)."
exit 1
fi
```

Disk Image Pre-Exec: Unmount a Disk Before a Raw Volume Backup

```
#!/bin/sh
echo "The disk will be unmounted!"
umount /disk_with_many_files
if [ $? = 0 ]
then
echo "The disk has been successfully unmounted!"
exit 0
```

```
else
echo "Failed to unmount the disk --> ABORTED!"
exit 1
fi
```

Filesystem Pre-Exec: Report Usage of the Filesystem

```
#!/bin/sh

echo
"================================================="
fuser -cu /var/application_mount_point
echo
"================================================="
exit 0
```

Session Post-Exec: Application Startup

This example Post-exec script will start up the Oracle database.

```
#!/bin/sh
export ORACLE_HOME=$2
export ORACLE_SQLNET_NAME=$1
if [ -f $ORACLE_HOME/bin/svrmgrl ]; then
        $ORACLE_HOME/bin/svrmgrl << EOF
connect sys/manager@$ORACLE_SQLNET_NAME as sysdba
startup
EOF
        echo "Oracle database \"$ORACLE_SID\" started."
        exit 0
else
        echo "Cannot find Oracle SVRMGRL
($ORACLE_HOME/bin/svrmgrl)."
        exit 1
```

```
fi
```

Disk Image Post-Exec: Mount a Disk After the Raw Volume Backup

```
#!/bin/sh
if [ $BDACC != 0]
then
echo "Backup could not read the disk!"
echo "Disk will not be automatically mounted!"
fi
echo "The disk will be now mounted!"
mount /dev/vg05/lvol2 /disk_with_many_files
if [ $? = 0 ]
then
echo "Disk successfully mounted!"
exit 0
else
echo "Failed to mount disk!"
exit 1
fi
```

Filesystem Post-Exec: Log Backup for the Record

```
#!/bin/sh
if  [ ! -f /etc/logfile ]
then
/etc/logfile
fi
echo "Backup finished with code $BDACC on " `date` >>
/etc/logfile
# We do not want a backup to be marked failed even if the
previous
action failed.
exit 0
```

Session Post-Exec: Notify User

```
#!/bin/sh
/opt/omni/bin/omnirpt -report single_session -session
$SESSIONID | \
 mailx -s "Report for $SESSIONID" $OWNER
```

Session Post-Exec: Start Another Backup

```
#!/bin/sh
# First check how the current backup finished
if [ $SMEXIT != 0 -o $SMEXIT != 10 ]
then
echo "Backup not successful --> next backup will not be
started!"
exit 0
fi
if  [ $RESTARTED != 0 ]
then
echo "Restarted backup --> next backup will not be
started!"
exit 0
fi
/opt/omni/bin/omnib -datalist BACKUP_NO_2 -no_mon
exit 0
```

Session Post-Exec: Restart Failed Backup

```
#!/bin/sh
# First check how the current backup finished
if [ $SMEXIT != 0 -o $SMEXIT != 10 ]
then
echo "Backup not successful --> backup will not be
restarted!"
exit 0
fi
if  [ $RESTARTED != 0 ]
```

```
then
echo "Restarted backup --> backup will not be
restarted!"
exit 0
fi
/opt/omni/bin/omnib -restart $SESSIONID -no_mon
exit 0
```

Disaster Recovery: Move Kill Links on HP-UX 11.x

Proceed as shown below on the system which you want to back up to move some links:

```
# The system will go from "run-level" 4 to "run-level 1"

# retaining the inetd, networking, swagentd services up.
The state is called "minimum activity" for backup
purposes (need networking).

# IMPORTANT: ensure the links are present in /sbin/rc1.d
before

# moving and they do have this exact name. You have to
rename them for the rc0.d directory. Put them BELOW the
lowest (original "/sbin/rc0.d/Kxx") "K...-link" in rc0.d

# Move K430dce K500inetd K660net K900swagentd into
../rc0.d BELOW the lowest kill link!!!

echo "may need to be modified for this system"

exit 1

#

cd /sbin/rc1.d

mv K430dce ../rc0.d/K109dce

mv K500inetd ../rc0.d/K110inetd

mv K660net ../rc0.d/K116net

mv K900swagentd ../rc0.d/K120swagentd
```

Creating a libaci.o on AIX

OmniBack II A.03.10 and Earlier

On AIX, Data Protector DAS Agent uses the object module `libaci.o` to access ADIC/GRAU system. This object module has to be created from the library archive file `libaci.a`, that is delivered by the vendor of ADIC/GRAU system.

1. Create the file `libaci.exp` containing the list of modules used by Data Protector DAS Agent:

```
#! /usr/omni/lib/libaci.o
aci_initialize
aci_qversion
aci_init
d_errno
aci_view
aci_drivestatus
aci_drivestatus2
aci_driveaccess
aci_mount
aci_dismount
aci_qvolsrange
aci_eject_complete
aci_eject
aci_insert
```

2. Create `libaci.o` by executing following command:

```
ld -L/usr/omni/lib -bM:SRE -e_nostart -lc
-bE:<DAS_PATH>/libaci.exp <DAS_PATH>/libaci.a -o libaci.o
```

   <DAS_PATH> is the path to the directory where `libaci.a` and `libaci.exp` files reside.

3. Copy `libaci.o` to the `/usr/omni/lib` directory.

OmniBack II A.03.5x and A.04.x

OmniBack II A.03.5x and A.04.x DAS Agent on AIX uses the library object module `named libaci.a` which has to be created from the library archive file of the same name. Proceed as follows to create the object module:

1. Create the file `libaci.exp` containing the list of modules used by the OmniBack II DAS Agent:

```
#! /usr/omni/lib/libaci.a
aci_initialize
aci_qversion
aci_init
d_errno
aci_view
aci_drivestatus
aci_drivestatus2
aci_driveaccess
aci_mount
aci_dismount
aci_qvolsrange
aci_eject_complete
aci_eject
aci_insert
```

2. Create the object module `libaci.o` by executing following command:

```
ld -L/usr/omni/lib -bM:SRE -e_nostart -lc
-bE:<DAS_PATH>/libaci.exp <DAS_PATH>/libaci.a -o libaci.o
```

   <DAS_PATH> is the path to the directory where the library archive file `libaci.a` and the `libaci.exp` files are located.

3. Copy the library object module `libaci.o` to the `/usr/omni/lib` directory and rename it to `libaci.a`.

IMPORTANT The full path to the library archive file is *<DAS_PATH>*`/libaci.a`, whereas the full path to the object module used by DAS Agent is `/usr/omni/lib/libaci.a`.

Example of the Package Configuration File

This section gives an example of a package configuration file that you need to modify while configuring Data Protector Cell Manager package in an MC/ServiceGuard environment:

```
**********************************************************************
********

# ****** HIGH AVAILABILITY PACKAGE CONFIGURATION FILE
(template) *******

#
**********************************************************************
********

# ******* Note: This file MUST be edited before it can be used.
********

# * For complete details about package parameters and how to
set them, *

# * consult the MC/ServiceGuard or ServiceGuard OPS Edition
manpages   *

# * or manuals.
*

#
**********************************************************************
********


# Enter a name for this package.  This name will be used to
identify the

# package when viewing or manipulating it.  It must be
different from

# the other configured package names.


PACKAGE_NAME ob2cl
```

```
# Enter the failover policy for this package. This policy will
be used
# to select an adoptive node whenever the package needs to be
started.
# The default policy unless otherwise specified is
CONFIGURED_NODE.
# This policy will select nodes in priority order from the list
of
# NODE_NAME entries specified below.
#
# The alternative policy is MIN_PACKAGE_NODE. This policy will
select
# the node, from the list of NODE_NAME entries below, which is
# running the least number of packages at the time this package
needs
# to start.

FAILOVER_POLICY CONFIGURED_NODE


# Enter the failback policy for this package. This policy will
be used
# to determine what action to take when a package is not
running on
# its primary node and its primary node is capable of running
the
# package. The default policy unless otherwise specified is
MANUAL.
# The MANUAL policy means no attempt will be made to move the
package
# back to its primary node when it is running on an adoptive
node.
#
# The alternative policy is AUTOMATIC. This policy will attempt
to
```

```
# move the package back to its primary node whenever the
primary node
# is capable of running the package.

FAILBACK_POLICY MANUAL


# Enter the names of the nodes configured for this package.
Repeat
# this line as necessary for additional adoptive nodes.
# Order IS relevant.  Put the second Adoptive Node AFTER the
first
# one.
# Example : NODE_NAME  original_node
#           NODE_NAME  adoptive_node

NODE_NAME partizan
NODE_NAME lyon


# Enter the complete path for the run and halt scripts.  In
most cases
# the run script and halt script specified here will be the
same script,
# the package control script generated by the cmmakepkg
command.  This
# control script handles the run(ning) and halt(ing) of the
package.
# If the script has not completed by the specified timeout
value,
# it will be terminated.  The default for each script timeout
is
# NO_TIMEOUT.  Adjust the timeouts as necessary to permit full
```

```
# execution of each script.
# Note: The HALT_SCRIPT_TIMEOUT should be greater than the sum
of
# all SERVICE_HALT_TIMEOUT specified for all services.

RUN_SCRIPT /etc/cmcluster/ob2cl/ob2cl.cntl
RUN_SCRIPT_TIMEOUT NO_TIMEOUT
HALT_SCRIPT /etc/cmcluster/ob2cl/ob2cl.cntl
HALT_SCRIPT_TIMEOUT NO_TIMEOUT


# Enter the SERVICE_NAME, the SERVICE_FAIL_FAST_ENABLED and the
# SERVICE_HALT_TIMEOUT values for this package.  Repeat these
# three lines as necessary for additional service names.  All
# service names MUST correspond to the service names used by
# cmrunserv and cmhaltserv commands in the run and halt
scripts.
#
# The value for SERVICE_FAIL_FAST_ENABLED can be either YES or
# NO.  If set to YES, in the event of a service failure, the
# cluster software will halt the node on which the service is
# running.  If SERVICE_FAIL_FAST_ENABLED is not specified, the
# default will be NO.
#
# SERVICE_HALT_TIMEOUT is represented in the number of seconds.
# This timeout is used to determine the length of time (in
# seconds) the cluster software will wait for the service to
# halt before a SIGKILL signal is sent to force the termination
# of the service.  In the event of a service halt, the cluster
# software will first send a SIGTERM signal to terminate the
# service.  If the service does not halt, after waiting for the
```

```
# specified SERVICE_HALT_TIMEOUT, the cluster software will
send
# out the SIGKILL signal to the service to force its
termination.
# This timeout value should be large enough to allow all
cleanup
# processes associated with the service to complete.  If the
# SERVICE_HALT_TIMEOUT is not specified, a zero timeout will be
# assumed, meaning the cluster software will not wait at all
# before sending the SIGKILL signal to halt the service.
#
# Example: SERVICE_NAME                  DB_SERVICE
#          SERVICE_FAIL_FAST_ENABLED     NO
#          SERVICE_HALT_TIMEOUT          300
#
# To configure a service, uncomment the following lines and
# fill in the values for all of the keywords.
#
#SERVICE_NAME                  <service name>
#SERVICE_FAIL_FAST_ENABLED     <YES/NO>
#SERVICE_HALT_TIMEOUT          <number of seconds>

SERVICE_NAME                  omni_sv
SERVICE_FAIL_FAST_ENABLED     NO
SERVICE_HALT_TIMEOUT          300


# Enter the network subnet name that is to be monitored for
this package.
# Repeat this line as necessary for additional subnet names.
If any of
```

```
# the subnets defined goes down, the package will be switched
to another

# node that is configured for this package and has all the
defined subnets

# available.


SUBNET 10.17.0.0



# The keywords RESOURCE_NAME, RESOURCE_POLLING_INTERVAL,

# RESOURCE_START, and RESOURCE_UP_VALUE are used to specify
Package

# Resource Dependencies.  To define a package Resource
Dependency, a

# RESOURCE_NAME line with a fully qualified resource path name,
and

# one or more RESOURCE_UP_VALUE lines are required.  The

# RESOURCE_POLLING_INTERVAL and the RESOURCE_START are
optional.

#

# The RESOURCE_POLLING_INTERVAL indicates how often, in
seconds, the

# resource is to be monitored.  It will be defaulted to 60
seconds if

# RESOURCE_POLLING_INTERVAL is not specified.

#

# The RESOURCE_START option can be set to either AUTOMATIC or
DEFERRED.

# The default setting for RESOURCE_START is AUTOMATIC.  If
AUTOMATIC

# is specified, ServiceGuard will start up resource monitoring
for

# these AUTOMATIC resources automatically when the node starts
up.
```

```
# If DEFERRED is selected, ServiceGuard will not attempt to
start

# resource monitoring for these resources during node start up.
User

# should specify all the DEFERRED resources in the package run
script

# so that these DEFERRED resources will be started up from the
package

# run script during package run time.

#

# RESOURCE_UP_VALUE requires an operator and a value.  This
defines

# the resource 'UP' condition.  The operators are =, !=, >, <,
>=,

# and <=, depending on the type of value.  Values can be string
or

# numeric.  If the type is string, then only = and != are valid

# operators.  If the string contains whitespace, it must be
enclosed

# in quotes.  String values are case sensitive.  For example,

#

# Resource is up when its value is

# --------------------------------

# RESOURCE_UP_VALUE= UP"UP"

# RESOURCE_UP_VALUE!= DOWNAny value except "DOWN"

# RESOURCE_UP_VALUE= "On Course""On Course"

#

# If the type is numeric, then it can specify a threshold, or a
range to

# define a resource up condition.  If it is a threshold, then
any operator

# may be used.  If a range is to be specified, then only > or
>= may be used
```

```
# for the first operator, and only < or <= may be used for the
second operator.
# For example,
# Resource is up when its value is
# --------------------------------
# RESOURCE_UP_VALUE     = 55    (threshold)
# RESOURCE_UP_VALUE     > 5.1greater than 5.1    (threshold)
# RESOURCE_UP_VALUE     > -5 and < 10between -5 and 10
(range)
#
# Note that "and" is required between the lower limit and upper
limit
# when specifying a range.  The upper limit must be greater
than the lower
# limit.  If RESOURCE_UP_VALUE is repeated within a
RESOURCE_NAME block, then
# they are inclusively OR'd together.  Package Resource
Dependencies may be
# defined by repeating the entire RESOURCE_NAME block.
#
# Example : RESOURCE_NAME
/net/interfaces/lan/status/lan0
#     RESOURCE_POLLING_INTERVAL120
#     RESOURCE_STARTAUTOMATIC
#     RESOURCE_UP_VALUE= RUNNING
#     RESOURCE_UP_VALUE= ONLINE
#
#           Means that the value of resource
/net/interfaces/lan/status/lan0
#         will be checked every 120 seconds, and is considered
to
#           be 'up' when its value is "RUNNING" or "ONLINE".
#
```

```
# Uncomment the following lines to specify Package Resource
Dependencies.

#

#RESOURCE_NAME     <Full_path_name>

#RESOURCE_POLLING_INTERVAL   <numeric_seconds>

#RESOURCE_START              <AUTOMATIC/DEFERRED>

#RESOURCE_UP_VALUE     <op> <string_or_numeric> [and <op>
<numeric>]



# The default for PKG_SWITCHING_ENABLED is YES. In the event of
a

# failure, this permits the cluster software to transfer the
package

# to an adoptive node.  Adjust as necessary.


PKG_SWITCHING_ENABLED YES



# The default for NET_SWITCHING_ENABLED is YES.  In the event
of a

# failure, this permits the cluster software to switch LANs
locally

# (transfer to a standby LAN card).  Adjust as necessary.


NET_SWITCHING_ENABLED YES



# The default for NODE_FAIL_FAST_ENABLED is NO.  If set to YES,

# in the event of a failure, the cluster software will halt the
node

# on which the package is running.  Adjust as necessary.
```

```
NODE_FAIL_FAST_ENABLEDNO
```

Example of the Package Control File

This section gives an example of a package control file that you need to modify while configuring Data Protector Cell Manager package in an MC/ServiceGuard environment:

```
**********************************************************************
********

# *
*

# *      HIGH AVAILABILITY PACKAGE CONTROL SCRIPT (template)
*

# *
*

# *      Note: This file MUST be edited before it can be used.
*

# *
*

#
**********************************************************************
********


# UNCOMMENT the variables as you set them.


# Set PATH to reference the appropriate directories.

PATH=/usr/bin:/usr/sbin:/etc:/bin


# VOLUME GROUP ACTIVATION:

# Specify the method of activation for volume groups.

# Leave the default ("VGCHANGE="vgchange -a e") if you want
volume

# groups activated in exclusive mode. This assumes the volume
groups have

# been initialized with 'vgchange -c y' at the time of
creation.
```

```
#
# Uncomment the first line (VGCHANGE="vgchange -a e -q n"), and
comment
# out the default, if your disks are mirrored on separate
physical paths,
#
# Uncomment the second line (VGCHANGE="vgchange -a e -q n -s"),
and comment
# out the default, if your disks are mirrored on separate
physical paths,
# and you want the mirror resynchronization to occur in
parallel with
# the package startup.
#
# Uncomment the third line (VGCHANGE="vgchange -a y") if you
wish to
# use non-exclusive activation mode. Single node cluster
configurations
# must use non-exclusive activation.
#
# VGCHANGE="vgchange -a e -q n"
# VGCHANGE="vgchange -a e -q n -s"
#VGCHANGE="vgchange -a y"
VGCHANGE="vgchange -a e"# Default


# VOLUME GROUPS
# Specify which volume groups are used by this package.
Uncomment VG[0]=""
# and fill in the name of your first volume group. You must
begin with
# VG[0], and increment the list in sequence.
#
# For example, if this package uses your volume groups vg01 and
vg02, enter:
```

Example of the Package Control File

```
#          VG[0]=vg01
#          VG[1]=vg02
#
# The volume group activation method is defined above. The
filesystems
# associated with these volume groups are specified below.
#
VG[0]=/dev/vg_ob2cm


# FILESYSTEMS
# Specify the filesystems which are used by this package.
Uncomment
# LV[0]=""; FS[0]=""; FS_MOUNT_OPT[0]="" and fill in the name
of your first
# logical volume, filesystem and mount option for the file
system. You must
# begin with LV[0], FS[0] and FS_MOUNT_OPT[0] and increment the
list in
# sequence.
#
# For example, if this package uses the file systems pkg1a and
pkg1b,
# which are mounted on the logical volumes lvol1 and lvol2 with
read and
# write options enter:
#          LV[0]=/dev/vg01/lvol1; FS[0]=/pkg1a;
FS_MOUNT_OPT[0]="-o rw"
#          LV[1]=/dev/vg01/lvol2; FS[1]=/pkg1b;
FS_MOUNT_OPT[1]="-o rw"
#
# The filesystems are defined as triplets of entries specifying
the logical
# volume, the mount point and the mount options for the file
system. Each
```

```
# filesystem will be fsck'd prior to being mounted. The
filesystems will be

# mounted in the order specified during package startup and
will be unmounted

# in reverse order during package shutdown. Ensure that volume
groups

# referenced by the logical volume definitions below are
included in

# volume group definitions above.

#

#LV[0]=""; FS[0]=""; FS_MOUNT_OPT[0]=""


LV[0]=/dev/vg_ob2cm/lv_ob2cm

FS[0]=/omni_shared

FS_MOUNT_OPT[0]=""


# FILESYSTEM UNMOUNT COUNT

# Specify the number of unmount attempts for each filesystem
during package

# shutdown.  The default is set to 1.

FS_UMOUNT_COUNT=2


# IP ADDRESSES

# Specify the IP and Subnet address pairs which are used by
this package.

# Uncomment IP[0]="" and SUBNET[0]="" and fill in the name of
your first

# IP and subnet address. You must begin with IP[0] and
SUBNET[0] and

# increment the list in sequence.

#

# For example, if this package uses an IP of 192.10.25.12 and a
subnet of
```

Example of the Package Control File

```
# 192.10.25.0 enter:
#          IP[0]=192.10.25.12
#          SUBNET[0]=192.10.25.0 # (netmask=255.255.255.0)
#
# Hint: Run "netstat -i" to see the available subnets in the
Network field.
#
# IP/Subnet address pairs for each IP address you want to add
to a subnet
# interface card.  Must be set in pairs, even for IP addresses
on the same
# subnet.
#
IP[0]=10.17.3.230
SUBNET[0]=10.17.0.0


# SERVICE NAMES AND COMMANDS.
# Specify the service name, command, and restart parameters
which are
# used by this package. Uncomment SERVICE_NAME[0]="",
SERVICE_CMD[0]="",
# SERVICE_RESTART[0]="" and fill in the name of the first
service, command,
# and restart parameters. You must begin with SERVICE_NAME[0],
SERVICE_CMD[0],
# and SERVICE_RESTART[0] and increment the list in sequence.
#
# For example:
#          SERVICE_NAME[0]=pkg1a
#          SERVICE_CMD[0]="/usr/bin/X11/xclock -display
192.10.25.54:0"
#          SERVICE_RESTART[0]=""  # Will not restart the
service.
```

```
#
#           SERVICE_NAME[1]=pkg1b
#           SERVICE_CMD[1]="/usr/bin/X11/xload -display
192.10.25.54:0"
#           SERVICE_RESTART[1]="-r 2"    # Will restart the
service twice.
#
#           SERVICE_NAME[2]=pkg1c
#           SERVICE_CMD[2]="/usr/sbin/ping"
#         SERVICE_RESTART[2]="-r 1" # Will restart the service
an infinite
#                                       number of times.
#
# Note: No environmental variables will be passed to the
command, this
# includes the PATH variable. Absolute path names are required
for the
# service command definition.  Default shell is /usr/bin/sh.
#
SERVICE_NAME[0]=omni_sv
SERVICE_CMD[0]="/etc/opt/omni/sg/csfailover.ksh start"
SERVICE_RESTART[0]="-r 2"
```

Data Protector Log Files Example Entries

This section provides some typical Data Protector messages that are logged to in some Data Protector log files. This section does not intended to provide further in-depth information on troubleshooting. For a complete list of Data Protector log files and for more in formation on them refer to "Data Protector Log Files" on page 550.

IMPORTANT The contents and format of entries to Data Protector log files are subject to change.

debug.log

```
02/11/00 12:22:01  OMNIRPT.23856.0
["/src/lib/cmn/obstr.c /main/r31_split/2":212] A.03.10
b325

  StrFromUserSessionId: "-detail": not in correct format


03/01/00 14:19:28  DBSM.21294.0
["PANSRC/db/RCS/cmn_srv.c,v 1.40":229] A.03.10 b325

  DB[1] internal error [9] cannot exclusively open
database, it is already opened


03/01/00 14:21:14  DBSM.21393.0
["PANSRC/db/RCS/cmn_srv.c,v 1.40":272] A.03.10 b325

  CDB cell server "bmw" different than current host
"bmw.hermes"


03/01/00 14:21:43  OMNIB.21471.0 ["/src/cli/omnibackup.c
/main/23":2585] A.03.10 b325

[Process] CanBackup failed!
```

```
03/02/00 09:36:51  INET.26130.0 ["/src/lib/ipc/ipc.c
/main/r31_split/10":6920] A.03.10 b325

IpcGetPeer: Could not expand ConnectionIP "10.17.6.227"


03/16/00 19:09:42  BSM.13152.0 ["src/db/cdb/cdbwrap.c
/main/84":1538] A.03.10 bPHSS_21234/PHSS_21235

  DB[1] internal error [-2009] The session is
disconnected


05/17/01 12:00:30  OMNIMM.7515.0 ["lib/cmn/obstr.c
/main/17":187] A.04.00.%B3 b335

  StrToUserSessionId: "0": not in correct format


5/14/01 11:08:53 AM  UPGRADE_CFG.357.356
["integ/barutil/upgrade_cfg/upgrade_cfg.c
/main/27":1472] A.04.00.%B3 b335

[UpgradeSQL] Can not read registry value
HKLM\Software\Hewlett-Packard\OpenView\OmniBackII\Agents
\MS-SQL70\saUser

[UpgradeSQL] Warning:  2, The system cannot find the
file specified.


5/14/01 11:08:54 AM  UPGRADE_CFG.369.368
["integ/barutil/upgrade_cfg/upgrade_cfg.c /main/27":154]
A.04.00.%B3 b335

[GetConfig] Can not read configuration from Cell Server
"brainiac.hermes" with integration "Oracle8" and
instance "_OB2_GLOBAL"

[GetConfig] Error: 1012, [12:1012] Can not access the
file.

System error: [2] The system cannot find the file
specified.
```

```
5/14/01 12:41:41 PM  OMNIDBUTIL.98.124
["db/vel_cls_spec.c /main/39":103] A.04.00.%B3 b335

  VELOCIS DB ERROR [0] internal error [-2005] Server
unavailable
```

sm.log

```
3/28/00 03:00:01  BSM.23475.0 ["/src/sm/bsm2/brsmutil.c
/main/r31_split/4":630] A.03.50.%B2 b158

Error connecting to database. Code: 1166.


03/27/01 08:17:06  BSM.2709.0 ["sm/bsm2/bsmutil.c
/main/502":3306] A.04.00.%B1 b281

Error opening datalist OMNIBACK-.
```

inet.log

```
5/15/01 12:19:54 AM  INET.119.122 ["inetnt/allow_deny.c
/main/10":524] A.04.00.%B3 b335

A request 3 came from host bmw.hermes which is not a Cell
Manager of this client


[Critical] From: INET@clio.hermes "clio.hermes"  Time:
03/29/01 09:48:29

[70:5]  Cannot execute '/opt/omni/lbin/ob2rman.exe' (No
such file or directory) => aborting
```

media.log

```
02/04/00 06:57:46 0a110210:3861cbbb:742d:0003 "[CBF492]
BMW_DLT_23" [2000/02/04-8] OmniDB


02/04/00 07:02:38 0a110210:3861cbbb:742d:0003 "[CBF492]
BMW_DLT_23" [2000/02/04-9]
```

DOC.
000233

CPL/AC

PREGÃO
050/2003

LOCAÇÃO DE EQUIPAMENTOS DE INFORMÁTICA INCLUINDO ASSISTÊNCIA TÉCNICA E TREINAMENTO

2003
PASTA 42

DEMAIS DOCUMENTOS

TERMO DE ENCERRAMENTO DO PROCESSO LICITATÓRIO

. CONTRATO ASSINADO
. PUBLICAÇÃO DO EXTRATO DE CONTRATO

RESULTADO DE JULGAMENTO
CARTA CONVITE Nº 1/2003

A Agência Nacional de Telecomunicações - Anatel, torna público o resultado da Carta Convite nº 001/2003/ANATEL-ER02. Processo nº 53508.001.049/2003, cujo objeto é a contratação de empresa especializada para execução de obra de engenharia destinada a preparar a infra-estrutura para implantação de uma Estação Remota de Radiomonitoragem (ERM), no Município de Volta Redonda - RJ., pelo período de 75 (setenta e cinco) dias, declarando vencedora a Empresa PLRG Construções e Aluguéis de Equipamentos LTDA. no valor total estimado de R$ 51.851,64 (cinquenta e um mil, oitocentos e cinquenta e um reais e sessenta e quatro centavos), pelo critério de menor preço. A presente contratação foi homologada pela Gerente Regional Substituta do RJ/ES em 29/10/2003.

GUSTAVO DENYS FERNANDES JULIO
Presidente da CPL

EMPRESA BRASILEIRA DE CORREIOS E TELÉGRAFOS
ADMINISTRAÇÃO CENTRAL

EXTRATOS DE CONTRATOS

A Empresa Brasileira de Correios e Telégrafos - ECT celebrou o seguinte contrato: Espécie: Contrato nº 12.126/2003; Data da Assinatura: 14/10/2003; Contratada: BARIZON Turismo e Arquitetura Ltda; Vigência 90 (noventa) dias a partir de 15/10/2003; Objeto: desenvolvimento e detalhamento dos projetos de arquitetura, projetos complementares, especificações técnicas, orçamentos analítico e sintético; Origem: Tomada de Preços Nº 001/2003- CPL/AC/ECT; Classificação Orçamentária: Projeto: 19.1.02, Conta: 3.04; Valor Total da Contratação: R$ 79.060,00 (setenta e nove mil e sessenta reais); Signatários: Eduardo Medeiros de Morais - Diretor de Tecnologia e de Infra-estrutura da Contratante e Jorge Dantas Dias - Chefe do Departamento de Infra-estrutura da contratante; Raymundo Barizon - Sócio Proprietário da contratada.

Contrato nº 12.162/2003; Data de assinatura: 28/10/2003; Contratada: RAFAEL INDÚSTRIA DE CONFECÇÕES LTDA; Objeto: Aquisição de Calça masculina e feminina para operador de triagem e transbordo: Origem: Pregão nº 073/2003 - CPL/AC; Vigência: Inicia na data de sua assinatura e termina com a entrega do último lote do material, fixado o prazo máximo de 6 (seis) meses; Classificação Orçamentária: Conta 2.02 e Atividade 00.8.00; Valor global: R$ 162.982,50; Signatários: Gabriel Pauli Fadel - Diretor de Administração e Adauto Tameirão Machado - Chefe do DECAM da Contratante: Antonio Nogueira Guerra - Representante da Contratada.

Contrato nº 12.163/2003; Data de assinatura: 28/10/2003; Contratada: RAFAEL INDÚSTRIA DE CONFECÇÕES LTDA; Objeto: Aquisição de Camisa para atendimento feminina, manga curta e longa: Origem: Pregão nº 070/2003 - CPL/AC; Vigência: Inicia na data de sua assinatura e termina com a entrega do último lote do material, fixado o prazo máximo de 6 (seis) meses; Classificação Orçamentária: Conta 2.02 e Atividade 00.8.00; Valor global: R$ 126.000,00; Signatários: Gabriel Pauli Fadel - Diretor de Administração e Adauto Tameirão Machado - Chefe do DECAM da Contratante; Antonio Nogueira Guerra - Representante da Contratada.

1. ESPÉCIE: Primeiro Termo Aditivo ao Contrato nº 11.994/03; 2. CONTRATADA: Hewlett-Packard Brasil Ltda; 3. OBJETO: Acréscimo de 13,46% do valor global do contrato, para prestação de serviços de locação e instalação de 119 servidores Intel Tipo 03 nas Diretorias Regionais; 4. VALOR DA ALTERAÇÃO: R$ 14.279.200,32; 5. DATA DE ASSINATURA: 03/10/2003; 6. VIGÊNCIA: A partir da assinatura até o limite da vigência do contrato original; 7. RECURSOS ORÇAMENTÁRIOS: Conta: 7.03 / Atividade: 00.8.00; 8. ORIGEM: REL/DITEC-PRT-018-021/2003; 9. SIGNATÁRIOS: Airton Langaro Dipp - Presidente da Contratante, Eduardo Medeiros de Morais - Diretor de Tecnologia e de Infra-Estrutura da Contratante, e Ivo Romani - Diretor da Contratada e José Eduardo Pires do Rio Ribeiro - Representante de Vendas da Contratada.

A Empresa Brasileira de Correios e Telégrafos celebrou o Contrato nº 12169/03 - Contratada: SOCIEDADE RÁDIO DIFUSORA ALEGRETENSE LTDA, assinado em 14/10/03 com vigência de 02 meses a partir da data de sua assinatura. Objeto: Contrato de Patrocínio Não-Incentivado. Origem: Inexigibilidade de Licitação nº 166/03. Conta orçamentária 00.8.00/5.02. Valor total da contratação: R$ 20.000,00 (vinte mil reais). Signatários: Airton Langaro Dipp - Presidente da Contratante e Gabriel Pauli Fadel - Diretor de Administração da Contratante; Samuel Marques da Silva - Diretora da Contratada

A Empresa Brasileira de Correios e Telégrafos - ECT celebrou Contrato com a seguinte firma:
01 - Espécie: Contrato nº 12.156/2003; Contratante: Empresa Brasileira de Correios e Telégrafos - ECT; Contratada: MICROTÉCNICA INFORMÁTICA LTDA; Vigência:a partir da data de assinatura e termina com a entrega do equipamento, limitado a 12 meses; Garantia: 12 meses a partir da emissão do Termo de Aceitação do equipamento; Objeto: aquisição de 01 impressora laser colorida, papel A3; Origem: Convite 18/2003 CPL/AC; Valor Global: R$ 22.885,00 (vinte e dois mil oitocentos e oitenta e cinco reais); Despesa orçamentária: Conta: 9.02. - Projeto: 17.1.06.: Signatários: Pela Contratante: GABRIEL PAULI FADEL - Diretor de Administração; Antônio Queiroz Pacheco - Chefe do Departamento de Suporte à Administração Central; Pela Contratada: ROBERTO MÁRCIO NARDES MENDES - Representante.

A Empresa Brasileira de Correios e Telégrafos celebrou o Contrato nº 12172/03 - Contratada: Associação Comercial e Industrial de Ijuí - ACI, assinado em 09/10/03 com vigência de 03 meses a partir da data de sua assinatura. Objeto: Contrato de Patrocínio Não-Incentivado. Origem: Inexigibilidade de Licitação nº 131/03. Conta orçamentária 00.8.00/5.02. Valor total da contratação: R$ 20.000,00 (vinte mil reais). Signatários: Airton Langaro Dipp - Presidente da Contratante e Gabriel Pauli Fadel - Diretor de Administração da Contratante; Jalmar José Martel - Presidente da Contratada.

1. ESPÉCIE: Contrato nº 12.168/03; 2. CONTRATADA: Gravoarte Clichês e Fotolitos Ltda; 3. OBJETO: Prestação de Serviços de Confecção e Gravação de 1.500 clichês-carimbos metálicos; 4. VALOR GLOBAL: R$ 21.000,00; 5. DATA DE ASSINATURA: 29/10/2003; 6. VIGÊNCIA: 29/10/2003 a 29/10/2004; 7. RECURSOS ORÇAMENTÁRIOS: Conta: 2.02 Atividade: 00.8.00; 8. ORIGEM: Convite nº 032/03; 9. SIGNATÁRIOS: Gabriel Pauli Fadel - Diretor de Administração da Contratante e Adauto Tameirão Machado - Chefe do Departamento de Contratação e Administração de Material da Contratante, e Gregório Augusto dos Santos Filho - Sócio- Proprietário da Contratada.

EXTRATO DE INEXIGIBILIDADE DE LICITAÇÃO

Inexigibilidade nº 175/03 - Data Autorização: 30/10/03 Objeto: Contrato de Patrocínio Não-Incentivado para realização do Projeto 9ª Olimpíada Internacional de Escolas Luteranas. Vigência: 03 meses a partir da data da assinatura do contrato entre a ECT e a Comunidade Evangélica Luterana São Paulo - CELSP - Valor total da contratação: R$ 18.000,00 (dezoito mil reais), pagos em parcela única no ano de 2003. - Caput do Art. 25 da Lei 8.666/93.

EXTRATOS DE TERMOS ADITIVOS

Terceiro Termo Aditivo ao Contrato 10.836/2001; Data de Assinatura: 18/10/2003; Contratada: VR Vales Ltda.; Vigência: 19/10/2003 a 18/10/2004, limitada à vigência do Contrato original; Objeto: Prorrogar a vigência do Contrato original por mais 12 meses; Classificação Orçamentária: Conta: 800.01.06.0000, Atividade: 00.8.00 - Infra-estrutura da ECT; Fundamentação: inciso II do Artigo 57 da Lei 8.666/93; Signatários: Airton Langaro Dipp - Presidente da Contratante -, Antônio Osório Menezes Batista - Diretor de Recursos Humanos da Contratante - e Cláudio Szajman - Presidente Executivo da Contratada.

1. ESPÉCIE: Primeiro Termo Aditivo ao Contrato nº 11.421/02; 2. CONTRATADA: MAXI GRÁFICA E EDITORA LTDA; 3. OBJETO: prorrogar a vigência do contrato por mais 12 (doze) meses, período de 02/10/2003 a 02/10/2004 e suprimir 60,45% do valor global inicialmente contratado; 4. VALOR DA SUPRESSÃO: R$ 217.000,00 5. DATA DE ASSINATURA: 01/10/2003; 6. RECURSOS ORÇAMENTÁRIOS: Conta: 00.8.00 - Atividade: 800.02.02.0000. 7. ORIGEM: Relatório/GCS/DGEC/DECAM-244/2003. 8. SIGNATÁRIOS: Airton Langaro Dipp - Presidente da Contratante, Gabriel Pauli Fadel - Diretor de Administração da Contratante, e Paulo César de Mesquita. - Diretor da Contratada.

AVISOS DE HOMOLOGAÇÃO DA ADJUDICAÇÃO
PREGÃO Nº 82/2003

Comunicamos a todos os interessados que o objeto do Pregão nº 082/2003 - CPL/AC, foi homologada a adjudicação à empresa LICENSE COMPANY INFORMÁTICA LTDA., para contratação de empresa especializada na operacionalização da modalidade Government Subscription da Microsoft -GS, para a cessão de direito de uso de seus softwares aplicativos, sistemas operacionais para estações de trabalho e software para equipamentos servidores, com o respectivo fornecimento de licenças e garantia de atualização das versões, no valor estimado de R$ 25.723.300,35 (vinte e cinco milhões e setecentos e vinte e três mil e trezentos reais e trinta e cinco centavos), para o período de 36 meses.

PREGÃO N.º 91/2003

Comunicamos a todos os interessados que o Registro de Preços, objeto do Pregão n.º 091/2003 - CPL/AC, foi homologada a adjudicação às empresas NOVADATA SISTEMAS E COMPUTADORES S/A (item 01), para Estação Convencional, no valor unitário de R$ 2.371,00 (dois mil e trezentos e setenta e um reais) e COMERCIAL STAR LTDA (itens 02 e 03), para Estação Gráfica no valor unitário de R$ 11.400,00 (onze mil e quatrocentos) e Estação de Desenvolvimento no valor unitário de R$ 5.900,00 (cinco mil e novecentos), respectivamente.

MARTA MARIA COELHO
Pregoeira

DIRETORIA REGIONAL EM ALAGOAS

EXTRATO DE CONTRATO

A ECT, através da GERAD/AL, efetuou o seguinte Contrato: Contrato n.º 140/2003; Data da assinatura: 30.09.2003; Locador: Maria José Pereira de Araújo; Prazo da Vigência: 01/10/2003 até 30/09/2004; Objeto do aditamento: Locação de imóvel para funcionamento da AC/Belém/AL; Valor total de desembolso: R$ 1.560,00 (Um mil e quinhentos e sessenta reais), Valor do desembolso no exercício: R$ 390,00 (trezentos e noventa reais) Origem: Dispensa de Licitação n.º 136/2003.

EXTRATO DE DISTRATO

A ECT, através da GERAD/DR/AL de comum acordo, efetuou o seguinte Distrato, a partir de 01/10/03: Distrato referente a Contrato n.º 083/1999; Data da assinatura: 30.09.2003; Locador: Creuza Albuquerque Lima; Objeto do Contrato original: Locação de Imóvel para funcionamento da AC/Chã Preta.

EXTRATO DE TERMO ADITIVO

A ECT, através da GERAD/AL, efetuou o seguinte Termo Aditivo: 1º Termo Aditivo ao Contrato de locação de imóvel nº 52/00 da AC/Santa Luzia do Norte/AL; Data da assinatura: 01.09.2003; Locador: Benedita O. Mascarenhas; Objeto do aditamento: Prorrogar a vigência do Contrato n.º 52/00 por mais um ano, pelo período de 01.09.03 a 31.08.04; Determinar que, durante o período acima, o referido instrumento contratual não sofrerá reajuste; Alterar o subitem 4.2., Clausula Quarta do Contrato, que passa a partir de 01/09/2003, a vigorar com a seguinte redação: A locatária efetuará o pagamento do aluguel, até o 5º (quinto) dia útil do mês subsequente, depositando a importância acordada no subitem 4.1. na Agência de Santa Luzia do Norte/AL, n.º 0389-1, Conta Corrente n.º 550.252-7, da locadora Sr. Benedita O. Mascarenhas; Objeto do contrato original: Locação de Imóvel para funcionamento da AC/Santa Luzia do Norte/AL

DIRETORIA REGIONAL NO ESPÍRITO SANTO

EXTRATOS DE TERMOS ADITIVOS

Termo aditivo ao contrato de prestação de serviços de manutenção preventiva e corretiva com aplicação de peças, nº 00316/2001, tem como objeto a renovação de vigência que terá início em 01/09/2003 e término em 31/08/2004 - Valor global R$ 15.336,00 (Quinze mil, trezentos e trinta e seis reais) Recursos orçamentários: Conta 3.17 Atividade 00.8.00 - Assinado em 26/09/2003.
Termo aditivo ao contrato de prestação de serviços de assistência técnica e manutenção preventiva e corretiva no elevador de carga nº 002-137/2000, tem como objeto alterar a Cláusula Quarta - subitem 4.1 e 4.2, em virtude de repactuação de preços - Valor global: R$ 5.052,00 (Cinco mil, cinquenta e dois reais): Recursos orçamentários: Conta 3.05 Atividade: 00.8.00 - Assinado em 19 de setembro de 2003.
Termo aditivo ao contrato de fornecimento de combustível (Gasolina comum, óleo diesel e álcool) para veículo do CDD-Cachoeiro de Itapemirim, nº 001-1025/2002, tem como objeto o acréscimo de 25% ao valor global - Valor global 66.677,25 (Sessenta e seis mil, seiscentos e setenta e sete reais e vinte e cinco centavos Recursos orçamentários: Conta 2.01 Atividade: 00.8.00 - Assinado em: 01 de outubro de 2003.

EXTRATOS DE CONTRATOS

Contrato nº 607/03; Data de Assinatura: 14/10/2003; Contratado: Divino Tavares Pereira - Vigência: inicia-se em 22/10/2003 e termina em 22/09/2004; Objeto: Locação de imóvel para funcionamento AC Córrego do Ouro/GO; Classificação Orçamentária: Atividade - 0800702.01; Valor da Contratação: R$ 4.200,00; Signatários: Sérgio Douglas Repolho Negri - Diretor Regional da Contratante, Valdblan Peres de Freitas - Presidente da CEL/DR/GT e Divino Tavares Pereira - Locador. Contrato nº 608/03; Data de Assinatura: 10/10/2003; Contratado: Antonio Rodrigues da Luz. Vigência: inicia-se em 10/10/2003 e termina em 10/10/2004; Objeto: Locação de imóvel para funcionamento AC São Francisco de Goiás/GO; Classificação Orçamentária: Atividade - 0800702.01; Valor da Contratação: R$ 3.360,00; Signatários: Sérgio Douglas Repolho Negri - Diretor Regional da Contratante, Valdblan Peres de Freitas - Presidente da CEL/DR/GT e Antonio Rodrigues da Luz - Locador. Contrato nº 609/03; Data de Assinatura: 10/10/2003; Contratado: Jasmiro Gonçalves de Almeida - Vigência: inicia-se em 10/10/2003 e termina em 10/10/2004; Objeto: Locação de imóvel para funcionamento AC Palestina de Goiás/GO; Classificação Orçamentária: Atividade - 0800702.01; Valor da Contratação: R$ 4.800,00; Signatários: Sérgio Douglas Repolho Negri - Diretor Regional da Contratante, Valdblan Peres de Freitas - Presidente da CEL/DR/GT e Jasmiro Gonçalves de Almeida - Locador. Contrato nº 611/03; Data de Assinatura: 10/10/2003; Contratado: Paulo Sergio Salvador - Vigência: inicia-se em 01/11/2003 e termina em 01/11/2004; Objeto: Locação de imóvel para funcionamento AC Palmeiropolis/TO; Classificação Orçamentária: Atividade - 0800702.01; Valor da Contratação: R$ 4.800,00; Signatários: Sérgio Douglas Repolho Negri - Diretor Regional da Contratante, Valdblan Peres de Freitas - Presidente da CEL/DR/GT e Paulo Sergio Salvador - Locador.

DIRETORIA REGIONAL EM GOIÁS E TOCANTINS

EXTRATO DE DISPENSA DE LICITAÇÃO Nº 362/200

Objeto: Locação de imóvel para funcionamento da AC Guaraíta/GO pelo período de 12 (doze) meses; Contratado: Célia de Morais Marques - CPF nº 363.561.151-49, com o valor global de R$ 2.880 (dois mil, oitocentos e oitenta reais), Data de assinatura: 20/10/2003 Vigência: Inicia-se em 21/10/2003 e termina em 2 /10/2004; Classificação orçamentária: 00800.07.02; Signatários: Sérgio Douglas Repolho Negri - Diretor Regional da Contratante, Valdblan Peres de Freitas - Presidente da Comissão Especial de Licitação - Célia Morais Marques - Locadora.

Ministério das Comunicações

SECRETARIA EXECUTIVA
SUBSECRETARIA DE PLANEJAMENTO, ORÇAMENTO E ADMINISTRAÇÃO

EXTRATO DE TERMO ADITIVO Nº 4/2004

Número do Contrato: 8/2000, Nº Processo: 53000.007193/1999. Contratante: MINISTERIO DAS COMUNICACOES. CNPJ Contratado: 03.520688000102. Contratado : APIS INTERNET CONSULTORIA E COMERCIO LTDA. Objeto: Prorrogar o prazo de vigência do Contrato n.º 08/2000-MC, pelo período de 12 meses, a contar de 28/2/2004. Fundamento Legal: Inciso II, do Art. 57, da Lein.º 8.666/93. Vigência: 28/02/2004 a 27/02/2005. Valor Total: R$ 6.790,00. Fonte: 174011059 - 2004NE900026. Data de Assinatura: 17/02/2004.

(SIDEC - 17/02/2004) 410003-00001-2004NE900079

AVISO DE LICITAÇÃO
PREGÃO Nº 2/2004

Aquisição de mobiliários e eletrodomésticos, destinados ao Centro das Comunicações Total de Itens Licitados: 00010 . Edital: 19/02/2004 de 08h00 às 12h00 e de 14h às 17h00 . Endereço: Esplanada dos Ministérios Bloco R, breloja, sala 126 Esplanada dos Ministérios - BRASILIA - DF . Entrega das Propostas: 04/03/2004 às 09:30 . Endereço: Esplanada dos Ministérios, bloco R,Auditório, térreo Esplanada dos Ministérios - BRASILIA - DF . Informações Gerais: Será cobrada a taxa de R$,00 (cinco reais) por edital.

JOSEMAR XAVIER ALVES
Pregoeiro

(SIDEC - 17/02/2004) 410003-00001-2004NE900079

AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES
SUPERINTENDÊNCIA DE ADMINISTRAÇÃO GERAL
GERÊNCIA-GERAL DE ADMINISTRAÇÃO

AVISO DE HOMOLOGAÇÃO
PREGÃO AMPLO Nº 67/2003

A Agência Nacional de Telecomunicações - Anatel, torna público o resultado da licitação de que trata o Edital de Pregão Amplo nº 67/2003, Processo nº 53500.005063/2003, cujo objeto é a aquisição de 9.600 (nove mil e seiscentas) resmas de papel para reprografia, no formato A4 (210 x 297 mm), na cor branca, 75g/m2, declarando vencedora a empresa Comercial Destro Ltda., no valor total de R$ 77.664,00 (setenta e sete mil seiscentos e sessenta e quatro reais). A presente contratação foi homologada pelo Gerente Geral de Administração, em 16.2.2004.

SÉRGIO LISBÔA FREIRE
Pregoeiro

GERÊNCIA DE MATERIAIS E CONTRATOS

EXTRATOS DE CONTRATOS

CONTRATO-APC-Nº 061/2003-ANATEL.
Data de Assinatura: 19 de dezembro de 2003; Contratada: ARMAZEM DIGITAL COMUNICAÇÃO E INFORMAÇÃO LTDA; Vigência: 19/12/2003 a 18/12/2004; Objeto: contratação de serviço de monitoramento de noticiário ("clipping") sobre o setor de telecomunicações, veiculado pelos principais meios de comunicação do país e no exterior, "Clipping" Mídia Impressa - jornal e revista, para disponibilização a todos os colaboradores da Anatel; Modalidade de Licitação: Pregão Amplo n.º 057/2003; Fundamentação Legal: artigos 55 e 57 da Lei n.º 9.472/97, Artigo 32 do Regulamento de Contratações, aprovado pela Resolução n.º 005/98-Anatel, e de modo subsidiário, pelas normas e procedimentos contidas no Regimento Interno da CONTRATANTE e de conformidade com a documentação constante do Processo n.º 53500.003798/2003; Programa de Trabalho: 24.122.0750.2000.0001, Elemento de Despesa: 33903900; Valor global anual do Contrato: R$ 40.999,20 (quarenta mil, novecentos e noventa e nove reais e vinte centavos); Nota de Empenho n.º 2003NE003179;Desembolso no Exercício: R$ R$ 3.416,60 (três mil, quatrocentos e dezesseis reais e sessenta centavos).

CONTRATO-ADGI-Nº 060/2003-ANATEL.
Data de Assinatura: 19 de dezembro de 2003; Contratada: JOSÉ LEITINO NETO - EPP; Vigência: 01/01/2004 a 31/12/2004; Objeto: fornecimento e entrega de jornais e revistas de comercialização em bancas de jornais, para o exercício de 2004, para os órgãos autorizados da sede da Anatel; Modalidade de Licitação: Pregão Amplo nº 72/2003; Fundamentação Legal: artigos 55 e 57, da Lei n.º 9.472/97, artigo 32 do Regulamento de Contratações, aprovado pela Resolução n.º 005/98-ANATEL, e de modo subsidiário, pelas normas e procedimentos contidas no Regimento Interno da CONTRATANTE e em conformidade coma documentação constante do Processo n.º 53500.005617/2003; Programa de Trabalho: 24.722.0750.2000.0001; Elemento de Despesa: 33903900; Valor total do Contrato: R$ 41.247,92 (quarenta e um mil, quatrocentos e quarenta e sete reais e noventa e dois centavos); Nota de Empenho n.º 2003NE003196; Desembolso no Exercício: R$ 3.000,00 (três mil reais).

EXTRATO DE TERMO ADITIVO

Quinto Termo Aditivo ao Contrato ADGSI Nº 010/2000-ANATEL; Data de Assinatura: 26 de janeiro de 2004; Contratada: Xerox Comércio e Indústria Ltda.; Vigência: 26/01/2004 a 25/01/2005; Objeto: Prorrogar vigência contratual pelo período de 12 (doze) meses; Fundamento Legal: O presente Aditamento está amparado no disposto do artigo 57, inciso II, da Lei n.º 8.666, de 21/06/93.

SUPERINTENDÊNCIA DE RADIOFREQUÊNCIA E FISCALIZAÇÃO
GERÊNCIA-GERAL DE FISCALIZAÇÃO
ESCRITÓRIO REGIONAL EM BELÉM

EXTRATO DE CONTRATO

Contrato ERIO (UO. 10.1) Nº 002/2004-ANATEL.
Data de Assinatura: 15 de janeiro de 2004.
Contratada: EMPRESA SENTINELA SERVIÇOS DE SEGURANÇA LTDA.
Vigência: 15/01/2004 À 14/01/2005.
Objeto: Prestação de serviços de vigilância física e patrimonial para atender a Unidade Operacional U.O 10.1, em São Luís/MA, pelo período de 12 (doze) meses, podendo ser prorrogado por igual período, até o limite de 60 (sessenta) meses.
Tipo de Licitação: Pregão Amplo
Fundamentação Legal: A presente contratação está amparada no disposto do art. 57, II, da Lei 8.666/93.
Programa de Trabalho: 24122075020020087.
Elemento de Despesa: 339039
Valor do Contrato: R$ 61.269,60 (sessenta e um mil, duzentos e sessenta e nove reais e sessenta centavos).
Nota de Empenho nº 2004NE000017.
Desembolso no Exercício: R$ 56.161,80 (cinqoenta e seis mil, cento e sessenta e um reais e oitenta centavos).

EMPRESA BRASILEIRA DE CORREIOS E TELÉGRAFOS
ADMINISTRAÇÃO CENTRAL

EXTRATOS DE CONTRATOS

1. ESPÉCIE: Contrato nº 12.527/2004; 2. CONTRATADA: CENTAURO - SERVIÇOS GRÁFICOS LTDA; 3. OBJETO: serviço gráfico de confecção e entrega de Folha de Etiqueta Auto-Adesiva com dados variáveis ; 4. VALOR GLOBAL: R$ 3.070.000,00 (três milhões e setenta mil reais) 5. DATA DE ASSINATURA: 03/02/2004; 6. VIGÊNCIA: 12 (doze) meses, com início a partir da assinatura, podendo ser prorrogado por 60 (sessenta) meses. 7. RECURSOS ORÇAMENTÁRIOS: Conta: 03.15 - Atividade/Projeto: 00.8.00. 8. ORIGEM: Pregão Eletrônico nº 117/2003 - CPL/AC 9. SIGNATÁRIOS: Eduardo Medeiros de Morais - Presidente da Contratante, Antônio Osório Menezes Batista - Diretor de Recursos Humanos respondendo pela Diretoria de Administração da Contratante, e Wedsley Ricky Bonventi - Representante da Contratada.ADAUTO TAMEIRÃO MACHADO/Chefe do Departamento de Contratação e Administração de Material/DECAM

1. ESPÉCIE: Contrato nº 12.533/2004; 2. CONTRATADA: ÁGUIA SISTEMAS DE ARMAZENAGEM S/A.; 3. OBJETO: aquisição de container aramado fixo - CAF-01; 4. VALOR GLOBAL R$ 1.176.000,00; 5. DATA DE ASSINATURA: 16/02/2004; 6. VIGÊNCIA: A partir da data de sua assinatura e termina com a entrega do último pedido, limitado ao prazo máximo de 12 meses; 7. RECURSOS ORÇAMENTÁRIOS: Projeto: 14.1.03 e Conta 9.02; 8. ORIGEM: Pregão nº 102/2003 - CPL/AC; 9. SIGNATÁRIOS: Eduardo Medeiros de Morais - Presidente da Contratante, Antônio Osório Menezes Batista - Diretor de Recursos Humanos, respondendo pela Diretoria de Administração da Contratante, Rogério Scheffer - Diretor Presidente da Contratada e João Francisco Miranda Ribas - Diretor Comercial e Industrial da Contratada.ADAUTO TAMEIRÃO MACHADO/Chefe do Departamento de Contratação e Administração de Material/DECAM

1. ESPÉCIE: Contrato nº 12.530/2004; 2. CONTRATADA: COMÉRCIO E INDÚSTRIA MULTIFORMAS LTDA; 3. OBJETO: serviço gráfico de confecção e entrega de Impressos de Segurança - Aerograma Simples, Envelope Pré-Pago e Telegrama Pré-pago ; 4. VALOR GLOBAL: R$ 1.289.000,00 (um milhão, duzentos e oitenta e nove mil reais) 5. DATA DE ASSINATURA: 13/02/2004; 6. VIGÊNCIA: 12 (doze) meses, com início a partir da assinatura, podendo ser prorrogado por 60 (sessenta) meses. 7. RECURSOS ORÇAMENTÁRIOS: Conta: 80.002.020.000 - Atividade/Projeto: 00.8.00. 8. ORIGEM: Pregão Eletrônico nº 124/2003 - CPL/AC 9 SIGNATÁRIOS: Eduardo Medeiros de Morais - Presidente da Contratante, Antônio Osório Menezes Batista - Diretor de Recursos Humanos respondendo pela Diretoria de Administração da Contratante, e Pedro Vieira da Silva - Representante da Contratada.ADAUTO TAMEIRÃO MACHADO/Chefe do Departamento de Contratação e Administração de Material/DECAM

EXTRATO DE CONVÊNIO

A ECT, por intermédio de sua Diretoria de Recursos Humanos, celebrou convênios de prestação de serviços de consignação em folha de pagamento com as seguintes Instituições Bancárias: 1- Convenio 001/2004; Assinado em: 28/01/2004, Banco BMG; Vigência a partir de 28/01/2003; 2- Convênio 002/2004, Assinado em: 28/01/2004; Banco Paulista; Vigência a partir de 28/01/2003.

EXTRATOS DE INEXIGIBILIDADE DE LICITAÇÃO

Inexigibilidade nº 05/04 - Data autorização: 16/02/04 - Objeto: Contrato de Patrocínio Não-Incentivado para realização do Projeto "EXPOBARRA 2004". Vigência: 03 meses a partir da data da assinatura do contrato entre a ECT e a Prefeitura Municipal de Barra Funda - Valor total da contratação= R$10.000,00 (dez mil reais), pagos em parcela única no ano de 2004 - Caput do Art. 25 da Lei 8.666/93.

Inexigibilidade nº 07/04 - Data autorização: 12/02/04 - Objeto: Contrato de Patrocínio Não-Incentivado para realização do Projeto "1º Seminário O Jovem e a Dependência Química". Vigência: 03 meses a partir da data da assinatura do contrato entre a ECT e o Centro Cultural e de Ação Social na Amazônia - CASA - Valor total da contratação: R$20.000,00 (vinte mil reais), pagos em parcela única no ano de 2004 - Caput do Art. 25 da Lei 8.666/93.

Inexigibilidade nº 14/04 - Data autorização: 10/02/04 - Objeto: Contrato de Patrocínio Não-Incentivado para realização do Projeto Documentários sobre o Programa Fome Zero. Vigência: 07 meses a partir da data da assinatura do contrato entre a ECT e a Caminho do Meio Criações Audiovisuais Ltda., - Valor total da contratação: R$47.000,00 (quarenta e sete mil reais) - Caput do Art. 25 da Lei 8.666/93.

EXTRATO DE TERMO ADITIVO

ESPÉCIE: Segundo Termo Aditivo ao Contrato nº 11.994/03; 2. CONTRATADA: Hewlett-Packard Brasil Ltda; 3. OBJETO: Substituir os produtos "Concord", objeto do Contrato, por produtos da HP da Família Open View, sem qualquer ônus para a CONTRATANTE, e alterar o subitem 5.1.2 da Cláusula Quinta; 4. DATA DE ASSINATURA: 30/01/2004; 5. VIGÊNCIA: Inicia-se na data de assinatura ficando limitada à vigência do contrato original; 6. ORIGEM: CI/DITEC/PRT-012 - 019/2003 e Rel/GCS/DGEC/DECAM-204/04, aprovado pelo Presidente em 30/01/2004; 7. SIGNATÁRIOS: Eduardo Medeiros de Morais - Presidente da Contratante e Paulo Roberto Menicucci - Diretor Comercial da Contratante, Ivo Romani - Diretor da Contratada e José Eduardo Pires do Rio Ribeiro - Representante de Vendas da Contratada.ADAUTO TAMEIRÃO MACHADO/Chefe do Departamento de Contratação e Administração de Material/DECAM

DIRETORIA REGIONAL DA BAHIA

EXTRATOS INSTRUMENTOS CONTRATUAIS

CTR 02/04 data da assinatura 21.01.04 - Contratado: Reinaldo de Lima Gomes Vigência: 01.02.04 à 01.02.05 - Objeto: Contratação de transportes de malas e malotes de natureza postal, na linha LCE-M-523 - AC Oliveira dos Brejinhos / Rodoviária Origem: DL-08/04 - valor global R$2.400,00 - Valor do desembolso R$2.000,00 Conta/atividade: 00.8.00-311-12 - 011.444.08.01.0012 - Enquadramento com base no art 24 da lei 8666/93 2) 3º Termo Aditivo ao CTR-116/99 - de prestação de serviços de manutenção preventiva corretiva de ar condicionado - Contratado: Tectenge Tecnologia e Serviços de Engenharia Ltda, resolvem de comum acordo, incluir novas disposições à cláusula 7ª ao subitens 7.5,7.6, 7.7 , 9º e revogar a cláusula 9º ao subitem 9.1 e 9.4, incluindo-se os subitens 9.5, ao subitem 9.1 e 9.4 - data da assinatura: 30.10.03 - 3) 2º Termo Aditivo ao CTR-04/03 de prestação de serviços de manutenção preventiva e corretiva em sistema de Ar condicionado com substituição de peças - Contratado: Plenum Instalações Ltda, alterar a cláusula 7ª ao subitem 7.1 e 9º ao subitem 9.1 data da assinatura: 23.12.03 - 4) 4º Termo Aditivo ao CTR-026/00 - Contrato de prestação de serviços de licenciamento e emplacamento de veículo da frota da ECT - Contratado: Edson dos Santos Saramandaia, alterar às cláusulas 3ª ao subitem 3.1, 4º ao subitem 4.1, 6º e 7º , subitem 7.1 - data da assinatura: 12.12.03 - 5) 1º Termo Aditivo ao CTR-155/03 de prestação de serviços de hotelaria - Contratado: Laj Empreendimentos Turísticos Ltda, alterar a cláusula 4ª ao subitem 4.1, 7º ao subitem 7.1.1b - data da assinatura: 03.12.03 - 6) 4º Termo Aditivo ao CTR - 134 A/01 de Locação de Imóvel onde funciona AC/Itaeté/Ba, - Locador: Telésphoro Azevedo Filho, alterar a cláusula 3º ao subitem 3.1 e 4º ao subitem 4.1 - 7) 3º Termo Aditivo ao CTR -416/00 de Locação de Imóvel onde funciona AC/Santa Bárbara/Ba Locador: Nelson José Estrela de Menezes, alterar a cláusula 3º ao subitem 3.1, 4º subitem 4.1 e o valor global - data da assinatura: 03.10.03 - 8) 4º Termo Aditivo ao CTR-114/02, de Transporte de Malas - Contratado: MM Transportes, alterar a cláusula 8ª ao subitem 8.1 e o valor global data da assinatura: 26.12.03 - 9) 8º Termo Aditivo ao CTR-08/00 de prestação de serviços limpeza e conservação - contratada: Lasev Conservação de Imóveis e Serviços Ltda, alterar a cláusula 3º ao subitem 3.1, 13º ao subitem 13.1, 15º ao subitem 15.1 - data da assinatura: 23.12.2003 - 10) 11º Termo Aditivo ao CTR - 044/00 de Transporte de Malas - Contratado: Rafer Transportes Rodoviário Ltda, alterar a cláusula 7º ao subitem 7.1 e 10º ao subitem 10.1 - data da assinatura: 19.01.04 - 11) 12º Termo Aditivo ao CTR-036/00 de Transporte de Malas, - contratada: Rafer Transportes Rodoviário Ltda, alterar a cláusula 7º ao subitem 7.1 e 10º ao subitem 10.1 - data da assinatura: 19.01.04 - 12) 3º Termo Aditivo ao CTR-137/00 de Locação de Imóveis onde funciona AC/Teofilândia/Bahia - Locador: Francisco José de Araújo Moura, alterar a cláusula 3º ao subitem 3.1 4º ao subitem 4.1 e o valor global - data da assinatura: 27.11.03 - 13) 3º Termo Aditivo ao CTR-146/01 de Locação de imóvel onde funciona AC/São Domingos/Ba - Locadores:

MAURICIO CESAR CANESTRARO	05020504114	514719149-68
MAURICIO EMERSON NUNES	05020730807	815845209-49
MAURICIO MARCELO NIENKOTTER	05020285137	610408949-68
MAURO APARECIDO BEZERRA DA SILVA	50011483750	027414219-86
MAVIAEL BATISTA DE MORAIS	09000048273	125825819-68
MIGUEL CRISTOVAM RODRIGUES	14020528551	398886499-49
NAGIBE CHEDE ABRAHAO	05000153251	000638009-34
NELSON FERREIRA BARRETO	50011172673	306132729-00
NELSON FOCK	14000035479	218494479-34
NELSON RACHED	05020734381	172319307-00
NELSON SCARDUA	50011741716	328564239-49
NEREU OLIVO	01000141357	000325570-00
NEY MUND FILHO	14020415510	417240549-53
NILO SILVA	14000065548	056815379-00
OLAIR MARCOS DA SILVA	50004680588	576703159-20
ORLANDO JOSE VARGAS	14020484406	050537909-06
OSMAR DE MORAES	14000012509	065941409-06
PACIFICO AMORIM	14000044702	255652499-53
PATRICIA VIEIRA BASTOS	50011257903	039949399-92
PAULO AUGUSTO DE MARI CASAGRANDE	05020751804	231089329-34
PAULO DOS SANTOS	50004353463	448594499-91
PAULO ERNESTO MIOTTO	50004139976	482064669-91
PAULO GODOY BECKER	05000159888	002718709-82
PAULO ROBERTO BRANDALIZE	05020545066	171000549-15
PAULO ROBERTO DA SILVA PEREIRA	05000200004	232605569-15
PEDRO FLORIANO VIEIRA	50002346346	487397409-78
PEDRO JOAO SCOTTON	50001721321	371153409-00
PEDRO PAULO CAMPOS	50004353382	494474169-34
PEDRO PAULO DOS SANTOS	14020527660	018276429-04
PETER SCHIRMER	05020742481	000000000-00
RAUL BUDAG	14020176850	076346171-72
RICARDO MACEDO BORIO	50011110643	366715099-72
RMM REPETIDORA MERCOSUL MEDIAN	50001866800	000000000-00
ROBERT ARMAINE BROOKS	05020728063	761671354-87
ROBERT JONCZYK	05000067410	004154069-78
TA ESPEZIM	14020433178	465305920-91
TO PINHEIRO	50011755261	786123739-72
ROSEMEIRE FERREIRA DE PAIVA	50012224782	048793749-03
ROSILEI VELHO	50004283902	092997328-33
RUBENS MANFRED BIAVATH	50004626885	296329559-04
RUBENS MARCELO BENATTI	05020637858	724262509-25
SANDRO POTYGUARA QUADROS	05020745588	015972549-67
SERGIO ELIAS DA SILVA NASCIMENTO	50011593695	620798329-72
SERGIO GILBERTO BONOCIELLI JUN	05020283860	043186578-76
SERGIO HENRIQUE OLIVEIRA DE CAMARGO	50001760572	717335669-53
SERGIO LUIS SMYTHE	05020733490	479353599-20
SERGIO ROBERTO BARBOSA REBELLATO	50005638089	186683649-87
SIDONIA KOPSCH DE MELO	50003619621	577041559-20
SIEGFRIED AUGUSTO HOHMANN	05000199081	002970549-53
SILVESTRE DOS SANTOS LIMA	05000128050	061795509-30
SIRLEI SALETE BASSO LOCATELLI	05020013994	663051529-34
SOLANO MEDINA FILHO	05020478792	026592049-34
SOLEMAR BORDIN	05020636290	357987509-49
SONIA MARIA APARECIDA LOPER	05000012275	003328619-10
TELMA PAULA DOS SANTOS	50012090050	847687549-53
TEREZINHA ELINEI DE OLIVEIRA	05000072090	028130259-68
THOMAZ DE AQUINO FILHO	02020396688	030746338-91
VALDONI MACEDO DA SILVA	14020428417	645931509-49
VALMOR SILVEIRA NETO	50004151402	019871929-90
VALNEIDE PODI	14020503052	613999499-34
VALTER DIAS DA SILVA	14020109826	097045319-15
VANADIR TEOFILO RIBEIRO	50011225203	286518559-15
VANDERLEI BITNER CARDOSO	50011573589	817456139-00
VERANI VIEIRA BASTOS	50011394226	728354279-53
VILSON ANTONIO ERN JUNIOR	14020476225	590857629-87
WALTER LUIZ VENSON	50011992980	759953369-91
WANDILINO WATERKEMPER	14000059491	104114709-06
WELINGTON MICHALAK	50010705627	186707849-04
WILSON JOSE DE SOUZA	05020566810	835122689-00

DIRCEU BARAVIERA
Gerente Geral de Serviços Privados de Telecomunicações

EMPRESA BRASILEIRA DE CORREIOS E TELÉGRAFOS
ADMINISTRAÇÃO CENTRAL

EXTRATO DE CONTRATO

A Empresa Brasileira de Correios e Telégrafos celebrou o Contrato nº 12668/04 - Contratada: SAGITARIUS RICK GARCIA PRODU-

EXTRATOS DE TERMOS ADITIVOS

1) 5º Termo Aditivo ao Contrato nº 11.123/2002; Assinatura: 03/04/2004; Contratado: Rodoviário União Ltda; Vigência: 03/04/2004 a 02/04/2005; Objeto: prorrogar o contrato 11.123/2002 por mais um período de 12 meses, sem repactuação de preços; valor global: 3.329.192,97; Classificação Orçamentária: Atividade 0800 - Conta: 311 04 02) 8º Termo Aditivo ao Contrato nº 11.124/2002; Assinatura: 03/04/2004; Contratado: Rodoviário União Ltda; Vigência: 03/04/2004 a 02/04/2005 ; Objeto: prorrogar o contrato 11.124/2002 por mais um período de 12 meses, sem repactuação de preços; valor global: 13.066.424,57; Classificação Orçamentária: Atividade 0800 - Conta: 311 04

1.ESPÉCIE: Sexto Termo Aditivo ao Contrato nº 10.640/01; 2. CONTRATADA: CTIS INFORMÁTICA LTDA; 3. OBJETO: prorrogação da vigência contratual por mais 12 (doze) meses, período de 02/05/2004 a 02/05/2005, e redução de aproximadamente 13% do valor global anual, em função da contratação específica em andamento para manutenção dos sistemas/ambiente legado (alta plataforma). 4. DATA DE ASSINATURA: 30/04/2004; 5. ORIGEM: CI/CIPRO - 088/2004, aprovado pelo DITEC em 01/04/2004; 6. SIGNATÁRIOS: João Henrique de Almeida Sousa - Presidente da Contratante, Eduardo Medeiros de Morais - Diretor de Tecnologia e de Infra-Estrutura da Contratante, Avaldir da Silva Oliveira - Diretor Geral da Contratada. 1.ESPÉCIE: Sétimo Termo Aditivo ao Contrato nº 10.641/01; 2. CONTRATADA: CTIS INFORMÁTICA LTDA; 3. OBJETO: prorrogação da vigência contratual por mais 12 (doze) meses, período de 02/05/2004 a 02/05/2005, e redução de aproximadamente 7% do valor global anual, em função da contratação específica em andamento para manutenção do ambiente legado (alta plataforma) e da descentralização do suporte técnico à computação pessoal para algumas Diretorias Regionais; 4. DATA DE ASSINATURA: 30/04/2004; 5. ORIGEM: CI/CIPRO - 088/2004, aprovado pelo DITEC em 01/04/2004; 6. SIGNATÁRIOS: João Henrique de Almeida Sousa - Presidente da Contratante, Eduardo Medeiros de Morais - Diretor de Tecnologia e de Infra-Estrutura da Contratante, Avaldir da Silva Oliveira - Diretor Geral da Contratada. 1.ESPÉCIE: Quarto Termo Aditivo ao Contrato nº. 10.642/01; 2. CONTRATADA: CTIS INFORMÁTICA LTDA; 3. OBJETO: prorrogação da vigência contratual por mais 12 (doze) meses, período de 02/05/2004 a 02/05/2005; 4. DATA DE ASSINATURA: 30/04/2004; 5. ORIGEM: CI/CIPRO - 088/2004, aprovado pelo DITEC em 01/04/2004; 6. SIGNATÁRIOS: João Henrique de Almeida Sousa - Presidente da Contratante, Eduardo Medeiros de Morais - Diretor de Tecnologia e de Infra-Estrutura da Contratante

1. ESPÉCIE: Terceiro Termo Aditivo ao Contrato nº 11.994/03; 2. CONTRATADA: HEWLETT-PACKARD BRASIL LTDA; 3. OBJETO: Acréscimo de 11,18% do valor global inicial do Contrato nº 11.994/2003, para prestação de serviços de locação e instalação de 39 (trinta e nove) servidores Intel Tipo 03 e 2 (dois) servidores RISC Tipo 01, novos de fábrica, incluindo configuração, assistência técnica e garantia; 4. DATA DE ASSINATURA: 28/04/2004; 5. RECURSOS ORÇAMENTÁRIOS: Conta: 80007030000 / Atividade: 00.8.00; 6. ORIGEM: Relatório/DITEC/DPROD-001/2004; 7. SIGNATÁRIOS: João Henrique de Almeida Sousa - Presidente da Contratante e Eduardo Medeiros de Morais - Diretor de Tecnologia e de Infra-Estrutura da Contratante, Carlos Rocha Ribeiro da Silva - Presidente da Contratada e José Eduardo Pires do Rio Ribeiro - Representante de Vendas da Contratada.

1. ESPÉCIE: Terceiro Termo Aditivo ao Contrato nº 11.419/02; 2. CONTRATADA: MAITRA INDÚSTRIA E COMÉRCIO DE ARTEFATOS DE PAPEL S/A; 3. OBJETO: Efetuar o acréscimo de 10% (dez por cento) sobre o valor global estimado do Contrato 11.419/2002, referente a prestação de serviços gráficos para produção de 600.000 (seiscentos mil) Envelopes CPF com janela; 4. DATA DE ASSINATURA: 06/05/2004; 5. RECURSOS ORÇAMENTÁRIOS: Conta: 800.03.15.0000 / Atividade: 00.8.00; 6. ORIGEM: CI/CVC/DVER/DEREV-0293/2004; 7. SIGNATÁRIOS: João Henrique de Almeida Sousa - Presidente da Contratante e Antônio Osório Menezes Batista - Diretor de Recursos Humanos, respondendo pela Diretoria de Administração da Contratante, e Silvio Rachid - Presidente da Contratada.

AVISOS DE HOMOLOGAÇÃO E ADJUDICAÇÃO
PREGÃO N.º 12/2004

Comunicamos a todos os interessados que o objeto do Pregão n.º 012/2004 - CPL/AC, foi homologada a adjudicação às empresas TRANSALL Equipamentos Industriais Ltda., para o fornecimento de 30 cabides de mala CM-03 (item 01) e MOVAP LTDA., para fornecimento de 109 cabides de malas CM-78 (item 02) , 194 racks para caixeta - RPC-01 (item 03), 213 racks para caixeta (item 04) e 500 suportes para caixeta - SC-01 (item 05), no valor total de R$ 288.278,00 (duzentos e oitenta e oito mil e duzentos e setenta e oito reais).

PREGÃO N.º 13/2004

Comunicamos a todos os interessados que o objeto do Pregão n.º 013/2004 - CPL/AC, foi homologada a adjudicação à empresa

DIRETORIA REGIONAL EM AMAZONAS E RORAIMA

EDITAL Nº 138/2004
PRORROGAÇÃO DE VALIDADE DE CONCURSO

A Empresa Brasileira de Correios e Telégrafos - ECT, Empresa Pública de direito privado, faz saber, que, de acordo com o disposto no Art. 37 III da Constituição Federal, estará prorrogando por mais um ano a validade do Concurso Público objeto do Edital nº 30/2003, realizado no dia 28 de janeiro de 2003, para o cargo de Técnico Operacional Júnior, na Diretoria Regional de Amazonas e Roraima, que teve seu resultado publicado no Diário Oficial da União no dia 12 de junho de 2003, seção 3, página 49.

PEDRO SÁTIRO DE ANDRADE
Presidente da Comissão Organizadora de Concurso Público

EDITAL Nº 139./2004
PRORROGAÇÃO DE VALIDADE DE CONCURSO

A Empresa Brasileira de Correios e Telégrafos - ECT, Empresa Pública de direito privado, faz saber, que, de acordo com o disposto no Art. 37 III da Constituição Federal, estará prorrogando por mais um ano a validade do Concurso Público objeto do Edital nº 27/2003, realizado no dia 27 de janeiro de 2003, para o cargo de Operador de Triagem e Transbordo, na Diretoria Regional de Amazonas e Roraima, que teve seu resultado publicado no Diário Oficial da União no dia 12 de junho de 2003, seção 3, página 44.

PEDRO SÁTIRO. DE ANDRADE
Presidente da Comissão Organizadora de Concurso Público

DIRETORIA REGIONAL NA BAHIA

AVISO DE HOMOLOGAÇÃO
PREGÃO Nº 4/2004

OBJETO: Sistema de Registro de Preços para aquisição de materiais de informática, com adjudicação do item 01 à empresa Áurea do Brasil Ltda, no valor global estimado de R$ 10.925,00 (dez mil, novecentos e vinte e cinco reais). Foi frustrada a compra dos itens 02(kit de carga/transferência p/ Lexmark T 610) e 03(Kit Fusor p/ Lexmark C710 10E0049).

EDLENA MARIA S. S. MACIEL
Pregoeira

DIRETORIA REGIONAL EM BRASÍLIA

AVISO DE REVOGAÇÃO
PREGÃO Nº 11/2004

A ECT, através da Diretoria Regional de Brasília, torna público a REVOGAÇÃO do Pregão 011/2004 (aquisição de gasolina comum no posto da contratada), tendo em vista o não comparecimento de nenhum interessado, caracterizando a licitação deserta.

EDSON PEREIRA DE CARVALHO
Pregoeiro

DIRETORIA REGIONAL NO ESPIRITO SANTO

EDITAL Nº143/2004

Com referência ao edital nº 66/2004, publicado no Diário Oficial da União de 22/03/2004, seção III, páginas 51 a 55, que trata da abertura do concurso público para os cargos de nível médio e superior, a Empresa Brasileira de Correios e Telégrafos, Diretoria Regional do Espírito Santo informa as seguintes retificações:

Onde se lê: 9.1. As provas objetivas constarão das disciplinas de Português, Matemática, Conhecimentos Específicos e Informática, num total de 50 questões.

Leia-se: 9.1.1. As provas objetivas constarão das disciplinas de Português, Matemática, Conhecimentos Específicos e Informática, num total de 40 questões.

ROSIANE TORRES SCANDIAN
Presidente da Comissão Organizadora de Concurso

DIRETORIA REGIONAL NO MATO GROSSO DO SUL

EXTRATO DE TERMO ADITIVO

NCIA NACIONAL DE TELECOMUNICAÇÕES
NTENDÊNCIA DE ADMINISTRAÇÃO GERAL
GERÊNCIA-GERAL DE ADMINISTRAÇÃO

XTRATO DE INEXIGIBILIDADE DE LICITAÇÃO

o nº 53500.003130/2003; Objeto: Contratação da Fundação sitária de Brasília - Fubra, para capacitação dos colaboradores ncia em cursos de extensão na regulação do setor de tele- cações, pelo período 18 (dezoito) meses; Valor total estimado: 79.600,00 (hum milhão quatrocentos e setenta e nove mil e tos reais); Amparo Legal: Inexigível a Licitação - art. 25, Inciso binado com o art. 13. inciso VI da Lei 8.666/93; Aprovação: tendente de Administração Geral; Ratificação: Presidente.

NCIA DE MATERIAIS E CONTRATOS

VISO DE LICITAÇÃO
NCORRÊNCIA Nº 1/2003

A Agência Nacional de Telecomunicações - Anatel, com o SAUS Quadra 06. Bloco "H", Edifício Ministro Sérgio Mot- cidade de Brasília -DF, Inscrita no CNPJ sob o nº .715/0001-12, torna público aos interessados que realizará li- na modalidade de Concorrência, no dia 17 de setembro de s 9 horas, cujo objeto é a concessão de uso remunerado de quipamentos e instalações próprias da Anatel, para exploração viço de lanchonete, com o fornecimento de lanches diversos, es rápidas e bombonieres, conforme Lei 8.666/93 e do Edital tará à disposição dos interessados a partir do dia 18/8/2003, no o Sede da Anatel, SAUS Quadra 06, Bloco "H", 3º andar - a - DF, no horário de 9 às 11 e das 15 às 17 horas ou fvel no site da Anatel, endereço: www.anatel.gov.br. Seção: teca - Licitações - Administrativas - Em Andamento.

ALENCASTRO GUIMARÃES DE BRITO
Presidente da Comissão Especial de Licitação

RESULTADO DO PREGÃO AMPLO Nº 51/2003

A Agência Nacional de Telecomunicações - Anatel, torna o o resultado da licitação de que trata o Edital de Pregão Amplo 2003, Processo nº 53500.003276/2003, cujo objeto é a produção latório Semestral da Ouvidoria, compreendendo a execução de ação eletrônica, confecção de projeto gráfico, diagramação, tra- to editorial, visual e gráfico, produção de fotolito e impressão 00 (mil) exemplares, declarando vencedora a empresa Quick Impressos Rápidos Ltda., no valor total de R$ 16.540,00 (de- s mil quinhentos e quarenta reais). A presente contratação foi ogada pelo Gerente de Materiais e Contratos, em 14.8.2003.

ALENCASTRO GUIMARÃES DE BRITO
Pregoeiro

.76/2003)

UPERI DÊNCIA DE RADIOFREQUÊNCIA E FISCALIZAÇÃO

AVISO DE LICITAÇÃO
PREGÃO AMPLO Nº 7/2003

O Escritório Regional da AGÊNCIA NACIONAL DE TE- OMUNICAÇÕES, no Rio Grande do Sul, estabelecido na Ave- Princesa Isabel, 778 - Porto Alegre - RS, Inscrita no CNPJ sob 02.030.715/0004-65, torna público aos interessados que realizará ão na modalidade de Pregão Amplo, no dia 29 de agosto de às 9:00 horas, cujo objeto é aquisição de material de consumo, nformidade com a Lei nº 9472/97 e o Regulamento de Con- ões da ANATEL, publicado no DOU de 19/01/98 e do Edital e nexo, que estará à disposição dos interessados a partir do dia 19 osto de 2003 neste Escritório Regional , 2º andar, sala 204 no eço acima citado, no horário das 9:00 as 12:00 e das 14 às 17:00 ou disponível no site da ANATEL , endereço : www.ana- v.br, opção: biblioteca/editais/editaisadm.htm.

WERLAU MENDES USSAM
Pregoeiro

EMPRESA BRASILEIRA DE CORREIOS E TELÉGRAFOS
ADMINISTRAÇÃO CENTRAL

EXTRATOS DE CONTRATOS

PÉCIE: Contrato nº 11.994/2003: 2.CONTRATANTE: EMPRE- BRASILEIRA DE CORREIOS E TELÉGRAFOS - ECT; CON- TADA: HEWLETT-PACKARD BRASIL LTDA; VALOR GLO- : R$ 106.036.869,19 (cento e seis milhões, trinta e seis mil, entos e sessenta e nove reais e dezenove centavos); RECURSOS AMENTÁRIOS: Conta: 07.03 Atividade: 00.8.00; DATA DA INATURA: 12/08/2003: VIGÊNCIA: O período de vigência se a na data da sua assinatura, prolongando-se até 48 (quarenta e meses), a contar da data da emissão do Termo de Aceitação da III; OBJETO: Prestação de Serviços de Locação e Instalação de (cento e sessenta e dois) equipamentos de informática - novos de ca - incluindo a configuração, o treinamento, a assistência técnica garantia, destinados aos Centros Corporativos de Dados da ECT, lizados nas cidades de Brasília e São Paulo; ORIGEM: Pregão nº /2003 - CPL/AC: SIGNATÁRIOS: Airton Langaro Dipp - Presidente da Contratante e Eduardo Medeiros de Morais - Diretor de tecnologia e Infra-estrutura da Contratante e José Eduardo Pires do Rio Ribeiro e Ivo Romani - Representantes da Contratada.

1.ESPÉCIE: Contrato nº 11.874/2003; 2.CONTRATANTE: EMPRESA BRASILEIRA DE CORREIOS E TELÉGRAFOS - ECT; CONTRATADA: AMERICAN BANKNOTE LTDA; VALOR GLOBAL: R$ 210.000,00 (duzentos e dez mil reais); RECURSOS ORÇAMENTÁRIOS: Conta: 3.07, Atividade: 03.2.20; DATA DA ASSINATURA: 20/06/2003; VIGÊNCIA: O período de vigência será de 12 (doze) meses, com início a partir da sua assinatura, podendo este prazo ser prorrogado até o cumprimento integral das obrigações contratadas, não excedendo a 60 (sessenta) meses ; OBJETO: Prestação de Serviços de Personalização de Selos Postais; ORIGEM: Pregão nº 010/2003 - CPL/AC; SIGNATÁRIOS: Gabriel Pauli Fadel - Diretor de Administração da Contratante e Adauto Tameirão Machado - Chefe do Departamento de Contratação e Administração de Material da Contratante e Sylio Ferreira Swerts e José Domingos Sidrim Bastos - Vice-Presidentes da Contratada.

1.ESPÉCIE: Contrato nº 11.995/2003; 2.CONTRATANTE: EMPRESA BRASILEIRA DE CORREIOS E TELÉGRAFOS - ECT; CONTRATADA: COMÉRCIO E INDÚSTRIA MULTIFORMAS LTDA; DATA DA ASSINATURA: 13/08/2003; VALOR GLOBAL: R$ 6.843.571,01 (seis milhões, oitocentos e quarenta e três mil, quinhentos e setenta e um reais e um centavo); RECURSOS ORÇAMENTÁRIOS: Atividade: 00.8.00 - Conta: 3.15; VIGÊNCIA: O período de vigência será de 12 (doze) meses, com início a partir de sua assinatura, podendo ser prorrogado por iguais e sucessivos períodos, limitados a 60 (sessenta) meses; OBJETO: Prestação de serviços gráficos; ORIGEM: Pregão n.º 44/2003 - CPL/AC; SIGNATÁRIOS: Airton Langaro Dipp - Presidente da Contratante e Gabriel Pauli Fadel - Diretor de Administração da Contratante e Pedro Vieira da Silva - Representante da Contratada.

01 - Espécie: Contrato 11986/03; Contratante: Empresa Brasileira de Correios e Telégrafos - ECT; Contratada: Esterilav Esterilização de Materiais Hospitalares Ltda EPP; Vigência: 12 (doze) meses, a partir de 01/08/2003; Objeto: prestação de serviços de lavanderia; Origem: Dispensa de Licitação número 335, de 24/07/2003; Valor Global: R$ 2.448,00 (dois mil e quatrocentos e quarenta e oito reais); Despesa orçamentária: Conta: 3.07 - Atividade: 00.5.05; Signatários: GABRIEL PAULI FADEL - Diretor de Administração, ANTÔNIO QUEIROZ PACHECO - Chefe do Departamento de Suporte à Administração Central - DESAD, Representantes da Contratante e MARIA DE FÁTIMA RABELO COSTA - Responsável Técnico da Contratada.

Contrato nº 11.985/2003; Data de assinatura: 12/08/2003; Contratada: Fax Point Indústria, Importação e Exportação Ltda; Objeto: Aquisição de 14.200 Cartuchos para Impressoras CANON; Origem: Pregão nº 037/2003 - CPL/AC; Vigência: Inicia na data de sua assinatura e termina com a entrega do último lote do material, limitada ao prazo máximo de 12 (doze) meses; Classificação Orçamentária: Conta 2.02 e Atividade 00.8.00; Valor total da Contratação: R$ 64.640,00; Signatários: Gabriel Pauli Fadel - Diretor de Administração da Contratante e Adauto Tameirão Machado - Chefe do Departamento de Contratação e Administração de Materiais da Contratante; Ellen Regina Maria de OLiveira - Representante da Contratada.

EXTRATOS DE TERMOS ADITIVOS

A Empresa Brasileira de Correios e Telégrafos - ECT celebrou Termo Aditivo com a seguinte firma: 01- Espécie: Primeiro Termo Aditivo ao Contrato nº 11.457/02; 02- Data de Assinatura:01/07/2003; 03- Contratada: AGÊNCIA ESTADO LTDA; 04- Objeto: prorrogação da vigência do Contrato por mais 12 (doze) meses, período de 02/07/2003 a 01/07/2004 e atualização do local de entrega das notas fiscais; 05- Signatários: Gabriel Pauli Fadel - Diretor de Administração e Antônio Queiroz Pacheco - Chefe do Departamento de Suporte a Administração Central, Representantes da Contratante, e João Bosco Ferreira Bastos - Diretor Regional e Ricardo Ferreira Bastos - Gerente Regional, Representantes da Contratada.

A Empresa Brasileira de Correios e Telégrafos - ECT celebrou Termo Aditivo com a seguinte firma: 01- Espécie: Primeiro Termo Aditivo ao Contrato nº 11.243/03, registrado sob nº 11.925/03; 02- Data de Assinatura: 17/07/2003; 03- Contratada: JCN INFORMÁTICA LTDA; 04- Objeto: correção de erro material ocorrido no subitem 2.6 da Cláusula Segunda do Contrato; 05- Signatários:Airton Langaro Dipp - Presidente e Gabriel Pauli Fadel - Diretor de Administração, Representantes da Contratante e José Valmir Paulino Dias - Sócio, Representante da Contratada.

AVISO DE ALTERAÇÃO
TOMADA DE PREÇOS Nº 1/2003

Alteramos o resultado do julgamento da habilitação da Tomada de Preços nº 001/2003-CPL/AC, publicado no DOU, Seção 03, pág. 41, do dia 25/06/2003, cujo objeto é o desenvolvimento de projetos executivos de arquitetura e dos complementares, referente a ampliação e adequação do Centro de Cartas e Encomendas de Benfica, na DR/RJ (item 01) e, reforma e adequação do 2º e 4º subsolos do Ed. Sede/ECT, em Brasília (item 02), da seguinte forma: empresa EPC Projetos e Construções Ltda., habilitada para o item 02.

TÂNIA REGINA TEIXEIRA MUNARI
Presidente da CPL

AVISO DE HOMOLOGAÇÃO E ADJUDICAÇÃO
PREGÃO Nº 54/2003

Comunicamos a todos os interessados que o objeto do Pregão n.º 054/2003 - CPL/AC, foi homologada a adjudicação à empresa FUNDAÇÃO CONESUL DE DESENVOLVIMENTO -FCD., para prestação de serviços de realização de concurso público, no valor global de R$ 49.855,00 (quarenta e nove mil e oitocentos e cinqüenta e cinco reais).

MARTA MARIA COELHO
Pregoeira

RETIFICAÇÃO

A Empresa Brasileira de Correios e Telégrafos, Departamento de Comunicação e Marketing, a Inex nº 061/03 - DPEV/DMARK, publicada no DOU do dia 15 de agosto de 2003, página 71, Seção 3, onde se lê: "Contratada Transnacional.com Ltda, assinado em 13/08/03...". Leia-se: - "Contratada Transnacional.com Ltda, assinado em 14/08/03...".

DIRETORIA REGIONAL EM ALAGOAS

EXTRATO DE TERMO ADITIVO

A ECT, através da GERAD/DR/AL, efetuou o seguinte Termo Aditivo: 1º Termo Aditivo ao contrato nº 041/2003; Data da assinatura: 30.07.2003: Contratada: Restaurante e Lanchonete Garry Kasparov Ltda; Prazo de vigência: 20.05.2003 até 19.05.2004; Objeto do aditamento: acrescer em 25% o valor global do contrato original passando de R$ 4.000,00 para 5.000,00; Objeto do contrato original: Prestação dos Serviços de coffee-break.

AVISO DE REVOGAÇÃO
PREGÃO Nº 6/2003

A ECT, Diretoria Regional de Alagoas, através do seu Pregoeiro e equipe de apoio, informa que a licitação relativa ao Pregão nº 006/2003, que visa a contratação de empresa para prestação de serviços de transporte de numerário em "carro-forte"(blindado), sob guarda de pessoal qualificado, fardado e armado foi Revogada.

ADILSON BATISTA LEITE
Pregoeiro

DIRETORIA REGIONAL NA BAHIA

AVISO DE LICITAÇÃO
PREGÃO Nº 11/2003

OBJETO: Aquisição de Formulário Contínuo. Abertura: 29/08/2003 às 09:30 horas, na Av. Paulo VI, 190, 4º andar - Pituba - Salvador/BA. Patrimônio Líquido: igual ou superior a R$33.350,00 (trinta e três mil, trezentos e cinqüenta reais) ou conforme Anexo I do Edital. Retirada de Edital: ECT Agência Pituba (Av. Paulo VI, 190 - Térreo) Salvador/BA, ao custo de R$5,00 (cinco reais), de 2ª à 6ª das 9 às 17 horas; sábado e domingo das 9 às 12 horas. Maiores informações: na CPL/DR/BA ou pelos telefones: (71)346-2720 ou fax: 346-2722.

EDLENA MARIA S.S. MACIEL
Pregoeira

DIRETORIA REGIONAL EM BRASÍLIA

EDITAL Nº 176 /2003

Convocação Para Prova Objetiva

A Empresa Brasileira de Correios e Telégrafos , por intermédio de sua Diretoria Regional de Brasília, em referência ao Edital 146/2003, torna público os locais onde serão aplicadas as Provas Objetivas, a serem realizadas no dia 24/08/2003, para provimento do cargo de Carteiro I.

A prova terá início às 14:00 horas e término às 18:00 horas.

Os candidatos deverão comparecer aos locais de provas com antecedência de 60 (sessenta) minutos, portando documento de identidade oficial (original).

O candidato que não receber a Carta de Convocação para Provas até o dia 20/08/2003, deverá fazer contato pelo telefone: (21) 2722-1815, sendo de sua responsabilidade tomar conhecimento de seu local de prova.

A relação dos locais de realização das provas bem como dos candidatos inscritos encontra-se disponível no site: www.correios.com.br .

MOACIR MAGALHÃES MARTINS
Presidente Regional da Comissão Organizadora do Concurso Público

Centro Educacional 02 Do Cruzeiro; Sbce/S A.805-Lote02-Area Esp. - C.Novo; Cruzeiro Novo; Brasilia; DF.

Centro Educacional Dimensao; QE 04 Area Especial C; Guara I; Brasilia; Df.

Centro De Ensino Medio Setor Oeste; SGAS 912/913, Modulo D.; Asa Sul; Brasilia; Df.

Centro De Ensino Medio Setor Leste; Sgas 611/12 L2 Sul; Asa Sul; Brasilia; Df.

Centro Educacional 01 Do Guara; Eq. 34/36 Area Especial Guara Ii; Guara Ii; Brasilia; Df.

Centro De Ensino Medio Taguatinga Norte; Qnc Area Especial 1 2 3; Norte; Brasilia; Df.

Centro Educacional Gisno; Sgan Qd. 907 Modulo A; Asa Norte; Brasilia; Df.

Centro Educacional 01 Do Cruzeiro; Area Especial F, Lote G; Cruzeiro Velho; Brasilia; Df.

TERMO DE CONTRATO

TERCEIRO TERMO ADITIVO AO CONTRATO Nº 11.994/03
PARA ACRÉSCIMO NA LOCAÇÃO E INSTALAÇÃO DE SERVIDORES

CONTRATANTE.....: EMPRESA BRASILEIRA DE CORREIOS E TELÉGRAFOS
CNPJ .....: 34.028.316/0001-03
INSCRIÇÃO ..... : 07.333.821/002-05
ENDEREÇO ..... : SBN, QD. 01 – CONJ. 3 - BLOCO A - ED. SEDE DA ECT
CEP..... : 70002-900 - Brasília - DF

PRESIDENTE.....: JOÃO HENRIQUE DE ALMEIDA SOUSA
IDENTIDADE.....: 808 – OAB/PI
CPF.....: 035.809.703-72

DEPARTAMENTO JURÍDICO
E C T
28 ABR 2004
Contrato nº 12664
BRASÍLIA - DF

DIRETOR DE TECNOLOGIA E
DE INFRA-ESTRUTURA .....: EDUARDO MEDEIROS DE MORAIS
IDENTIDADE.....: 453.609 – SSP/DF
CPF.....: 150.199.771-87

CONTRATADA.....: HEWLETT-PACKARD BRASIL LTDA
CNPJ.....: 61.797.924/0001-55
INSCRIÇÃO ESTADUAL....: 206.203.572.117
ENDEREÇO.....: AL. RIO NEGRO, 750 – ALPHAVILLE –
CEP: 06454-000 - BARUERI/SP
TELEFONE.....: (11) 4197-8000
FAX.....: (11) 4197-8432

RQS nº 05/2005 - CN -
CPMI - CORREIOS
Fls: 0980
3685
Doc:

REPRESENTANTES

PRESIDENTE..... : CARLOS ROCHA RIBEIRO DA SILVA
IDENTIDADE.....: 17.817.822 SSP/SP
CPF.....: 405.086.097-04

REPRESENTANTE DE VENDAS.....: JOSÉ EDUARDO PIRES DO RIO RIBEIRO
IDENTIDADE.....: 15.319.247 SSP/SP
CPF.....: 071.885.858-14

DEPARTAMENTO JURÍDICO E C T
Conforme
NJ/DEJUR/DJRAD 34/04

CLÁUSULA PRIMEIRA - DO OBJETO

1.1. O presente Termo Aditivo tem por objeto o acréscimo de 11,18% (onze vírgula dezoito por cento) do valor global inicial do Contrato nº 11.994/2003, para prestação de serviços de locação e instalação de **39 (trinta e nove) servidores Intel Tipo 03** e **2 (dois) servidores RISC Tipo 01**, novos de fábrica, incluindo a configuração, assistência técnica e garantia, conforme quantidades, locais de entrega e modelos descritos no **Anexo I** e Especificações Técnicas descritas no Anexo 1-B do Contrato e Anexo 1 do Primeiro Termo Aditivo.

CLÁUSULA SEGUNDA – DO SERVIDOR RISC TIPO 01

2.1. Os Servidores RISC Tipo 01, objeto deste Termo Aditivo, serão entregues com tecnologia "ITANIUM", conforme Carta da CONTRATADA, datada de 12 de Abril de 2004 e Parecer Técnico/DPROD-318/2004.

CLÁUSULA TERCEIRA – DO CRONOGRAMA DE EXECUÇÃO

3.1. A Contratada deverá obedecer o seguinte cronograma de execução :

Fase	Descrição	Prazo(dias)
I	Entrega, Instalação e Configuração dos Equipamentos em até	D + 30
II	Aceitação Final dos Equipamentos em até	D + 30

(Onde D = Data de Assinatura deste Instrumento) :

CLÁUSULA QUARTA – DO PREÇO E PAGAMENTO

4.1. O preço de locação mensal é, por servidor INTEL Tipo 03 locado, R$ 2.499,86 (dois mil quatrocentos e noventa e nove reais e oitenta e seis centavos). Para os 39 (trinta e nove) servidores adicionais, locados por este Termo Aditivo, o preço mensal da locação será de R$ 97.494,54 (noventa e sete mil, quatrocentos e noventa e quatro reais e cinqüenta e quatro centavos).

4.2. O preço de locação mensal é, por servidor RISC Tipo 01 locado, R$ 95.724,89 (noventa e cinco mil, setecentos e vinte e quatro reais e oitenta e nove centavos). Para os 2 (dois) servidores adicionais, locados por este Termo Aditivo, o preço mensal da locação será de R$ 191.449,78 (cento e noventa e um mil, quatrocentos e quarenta e nove reais e setenta e oito centavos).

4.3. O valor da totalidade dos servidores locados por este Termo Aditivo, relativo a 41 (quarenta e um) meses de alugueres, é R$ 11.846.717,12 (onze milhões, oitocentos e quarenta e seis mil, setecentos e dezessete reais e doze centavos).

4.4. Os pagamentos serão efetuados mediante a apresentação de Nota(s) Fiscal(is)/Fatura(s) para a Diretoria Regional de São Paulo Metropolitana ou para a Administração Central, conforme o servidor locado, nos locais descritos no **Anexo I**, devidamente atestada(s) pela **CONTRATANTE**, mensalmente durante os **41 (quarenta e um)** meses de alugueres, no **15º (décimo quinto) dia** do mês subseqüente ao da prestação dos serviços , após a emissão do **Termo de Aceitação,** da Fase II, descrita no subitem 3.1.

CLÁUSULA QUINTA – DO PERÍODO DE GARANTIA DE FUNCIONAMENTO

5.1. O período de vigência da garantia de funcionamento dos equipamentos será de **41 (quarenta e um) meses**, contados a partir da data do aceite da Fase II deste Termo Aditivo.

CLÁUSULA SEXTA – DA GARANTIA DE EXECUÇÃO

6.1. A **CONTRATADA** comprovará no prazo de **05 (cinco) dias úteis** da data de assinatura deste Termo Aditivo, a efetivação da garantia de execução contratual, que deverá corresponder à vigência do presente Instrumento, em percentual equivalente a **3% (três por cento)** do valor da alteração, correspondente a **R$ 355.401,51** (trezentos e cinqüenta e cinco mil, quatrocentos e um reais e cinqüenta e um centavos), podendo optar por uma das seguintes modalidades :

a) caução em dinheiro ou títulos da dívida pública;
b) seguro-garantia;
c) fiança bancária.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls: 0982
3685

6.2. Em caso de garantia em dinheiro, a **CONTRATADA** deverá depositar o valor em nome da **CONTRATANTE** , conforme dados abaixo :

DEPARTAMENTO JURÍDICO DEJUR
Conforme
MJ/DEJUR/DJRAO 35404

BANCO: Banco do Brasil S.A. (001)
AGÊNCIA: 3307-3
CONTA CORRENTE: 195.159-9

CLÁUSULA SÉTIMA – DO VALOR DA ALTERAÇÃO

7.1. O aditamento em questão implicará em acréscimo de R$ 11.846.717,12 (onze milhões, oitocentos e quarenta e seis mil, setecentos e dezessete reais e doze centavos) no valor global do Contrato nº 11.994/2003.

CLÁUSULA OITAVA - DO VALOR GLOBAL

8.1 O valor global do Contrato nº 11.994/2003, acrescido do valor deste aditivo, passará a ser de R$ 132.162.786,63 (cento e trinta e dois milhões, cento e sessenta e dois mil, setecentos e oitenta e seis reais e sessenta e três centavos).

CLÁUSULA NONA – DOS RECURSOS ORÇAMENTÁRIOS

9.1. As despesas decorrentes da prestação de serviços, objeto deste aditamento, correrão por conta da seguinte classificação orçamentária :

Conta: 80007030000 - Atividade: 00.8.00

CLÁUSULA DÉCIMA – DA VIGÊNCIA

10.1. O presente Termo Aditivo vigorará a partir da data de sua assinatura até o limite da vigência do Contrato original.

CLÁUSULA DÉCIMA-PRIMEIRA – DA FUNDAMENTAÇÃO LEGAL E DA AUTORIZAÇÃO

11.1. O presente Termo Aditivo tem respaldo no subitem 2.11 da Cláusula Segunda e no subitem 7.1.1, alinea "b" da Cláusula Sétima do Contrato nº 11.994/2003 e na Lei nº 8.666/93, Artigo 65, Inciso I, Alínea "b" e Parágrafo 1º .

DEPARTAMENTO JURÍDICO E T
Conforme
MJ/DEJUR/DJRAD 354/04

11.2. O presente aditamento foi autorizado conforme Relatório/DITEC/DPROD nº 001/2004, aprovado pelo Presidente da ECT em 15/04/2004.

CLÁUSULA DÉCIMA-SEGUNDA – DA RATIFICAÇÃO

12.1. Ficam ratificadas as demais cláusulas e condições do Contrato Original, que não conflitem com as alterações ora acordadas.

E, por estarem justas e acordadas, as partes assinam o presente Termo Aditivo em **02 (duas) vias** de igual teor e forma e para um só efeito, na presença das testemunhas abaixo assinadas.

Brasília/DF, 28 de abril de 2004.

PELA CONTRATANTE:

JOÃO HENRIQUE DE ALMEIDA SOUSA
Presidente

EDUARDO MEDEIROS DE MORAIS
Diretor de Tecnologia e de Infra-Estrutura

PELA CONTRATADA:

CARLOS ROCHA RIBEIRO DA SILVA
Presidente

JOSÉ EDUARDO PIRES DO RIO
Representante de Vendas

TESTEMUNHAS:

1. _____
Nome: Eduardo Henrique Peres
CPF: 488866530-34

2. _____
Nome: Jacinunes Carneiro Jorge
CPF: 249.124.681-34

RQS nº 03/2005 - CN
CPMI - CORREIOS
0984
Fls:
3685
Doc:

DEPARTAMENTO JURÍDICO E T
Conforme
NJ/DEJUR/BJRAO 354/04

Anexo 1

1. PAUTA DE DISTRIBUIÇÃO:

	Tipo de servidor	
Localidade	**Intel Tipo 03**	**RISC Tipo 01**
Administração Central	22	02
Diretoria Regional de São Paulo - Metropolitana	17	Zero

2. ENDEREÇOS PARA ENTREGA E MANUTENÇÃO DOS EQUIPAMENTOS:

Localidade	Endereço	Telefones
Administração Central	SBN – Quadra 01, Conjunto 03, Bloco A, Ed. Sede dos Correios CEP: 70002-900 – Brasília/DF	(61) 426-2214 (61) 426-1754 Fax (61) 426-2206
Diretoria Regional de São Paulo - Metropolitana	Rua Mergenthaler, 592 – Bl.2 – Vila Leopoldina CEP: 05311-900 – São Paulo/SP	(11)3838-7700 Fax: (11)3838-1599

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls: 0985
Doc: 3685

DEPARTAMENTO JURÍDICO E C T
Conforme
NJ/BEJUR/DJRAD 354/04

SEGUNDO TERMO ADITIVO AO CONTRATO Nº 11.994/03

CONTRATANTE: EMPRESA BRASILEIRA DE CORREIOS E TELÉGRAFOS

CNPJ.....: 34.028.316/0001-03
INSC. ESTADUAL.....: 07.333.821/002-05
ENDEREÇO.....: SBN - Quadra 01 – Bl. "A" 6º Andar Ed. Sede da ECT
CEP.....: 70002-900 BRASÍLIA-DF

REPRESENTANTES:

PRESIDENTE..... : EDUARDO MEDEIROS DE MORAIS
IDENTIDADE..... : 453.609-SSP/DF
CPF..... : 150.199.771-87

DIRETOR COMERCIAL..... : PAULO ROBERTO MENICUCCI
IDENTIDADE..... : M-53.430 -SSP/MG
CPF..... : 011.092.276-04

DEPARTAMENTO JURÍDICO
E C T
30 JAN 2004
Contrato nº 12521
BRASÍLIA - DF

CONTRATADA: HEWLETT-PACKARD BRASIL LTDA

CNPJ .....: 61.797.924/0001-55
INSCRIÇÃO ESTADUAL.....: 206.203.572.117
ENDEREÇO.....: AL. RIO NEGRO, 750 – ALPHAVILLE – BARUERI/SP
CEP.....: 06454-000
FONE.....: (11) 4197-8000
FAX.....: (11) 4197-8432

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls: 0986
Doc: 3685

REPRESENTANTES:

DIRETOR.....: IVO ROMANI
IDENTIDADE.....: 7.187.356-9 - SSP/SP
CPF.....: 903.621.798-91

HEWLETT PACKARD JURÍDICO

REPRESENTANTE DE VENDAS.....: JOSÉ EDUARDO PIRES DO RIO RIBEIRO
IDENTIDADE.....: 15.319.247 - SSP/SP
CPF.....: 071.885.858-14

DEPARTAMENTO JURÍDICO E C T

Conforme
Nº DEJUR/DJTEC ...../.....

CLÁUSULA PRIMEIRA - DO OBJETO

1.1. O presente Termo Aditivo tem por objeto alterar os seguintes pontos do Contrato 11.994/03:

a) Substituir os produtos "Concord", objeto do Contrato, por produtos da HP da Família Open View, sem qualquer ônus para a CONTRATANTE;

b) Alterar o subitem 5.1.2 da Cláusula Quinta.

CLÁUSULA SEGUNDA – ACORDO DE SUBSTITUIÇÃO DE SOFTWARES

2.1. Acordam as partes em substituir, sem quaisquer ônus adicionais à CONTRATANTE, os produtos "Concord" objeto do Contrato, por produtos HP da família Open View.

CLÁUSULA TERCEIRA – ITEM 5.1.2 DO CONTRATO Nº 11.994/03

3.1. O item mencionado passará a ter a seguinte redação:

- ***Subitem 5.1.2 – "mensalmente referente aos 48 (quarenta e oito) meses de alugueres, no 20º (vigésimo) dia do mês subseqüente ao da prestação dos serviços, após a emissão do Termo de Aceitação Fase III, conforme descrito no ANEXO 1-A deste Contrato.***

3.2. Em razão da alteração informada acima, fica alterado o período de emissão das faturas das parcelas inicial, com vencimento em 20/12/2003, compreendendo o período de 29/10/2003 a 29/11/2003, e final, com vencimento em 20/11/2007, compreendendo o período de 29/09/2007 a 29/10/2007, do aluguel de equipamentos.

REQ Nº 05/2005 - CN - CPMI - CORREIOS
Fls: 0987
3685
Doc:

CLÁUSULA QUARTA – DA VIGÊNCIA

4.1. A vigência do presente Termo Aditivo inicia-se na data de sua assinatura ficando limitada à vigência do contrato original.

HEWLETT PACKARD JURÍDICO

CLÁUSULA QUINTA – DA AUTORIZAÇÃO

5.1. O presente Instrumento foi aprovado pelo Presidente da ECT, por meio do **Relatório/GCS/DGEC/DECAM- 204/2004.**

DEPARTAMENTO JURÍDICO E C T

Conforme
NJ/DEJUR/DJTEC ...../...../.....

CLÁUSULA SEXTA - DA FUNDAMENTAÇÃO E SUBORDINAÇÃO LEGAL

6.1. O presente Instrumento tem respaldo legal na Lei 8.666/93 (Artigo 65, Inciso I, alínea "a").

CLÁUSULA SÉTIMA - DA RATIFICAÇÃO

7.1. Ficam ratificadas todas as demais Cláusulas, itens e condições do Contrato Original, que não conflitarem com o presente Instrumento.

E, por estarem justas e acordadas, as partes assinam, o presente Termo Aditivo em 02 (duas) vias de igual teor e forma e para um só efeito, na presença das testemunhas abaixo assinadas.

Brasília/DF, 30 de janeiro de 2004.

PELA CONTRATANTE

EDUARDO MEDEIROS DE MORAIS
Presidente

PAULO ROBERTO MENICUCCI
Diretor Comercial

PELA CONTRATADA

IVO ROMANI
Diretor

JOSÉ EDUARDO PIRES DO RIO RIBEIRO
Representante de Vendas

HEWLETT-PACKARD JURÍDICO

TESTEMUNHAS:

1) _____
Nome: Yane Carvalho
CPF: 833594351-68

2) Daniele Rosa de Alcântara
Nome:
CPF: 334.038.131-34

DEPARTAMENTO JURÍDICO
Conforme
MJ DEJUR/DJTEC

RQS nº 03/2005 - CN - CPMI - CORREIOS
0988
Fls: 1
Doc: 3685

PRIMEIRO TERMO ADITIVO AO CONTRATO Nº 11.994/03
PARA ACRÉSCIMO NA LOCAÇÃO E INSTALAÇÃO DE SERVIDORES

CONTRATANTE : EMPRESA BRASILEIRA DE CORREIOS E TELÉGRAFOS
CNPJ : 34.028.316/0001-03
INSCRIÇÃO : 07.333.821/002-05
ENDEREÇO : SBN, QUADRA 01 – CONJ.3 - BLOCO A - ED. SEDE DA ECT
CEP. : 70002-900 - Brasília - DF

PRESIDENTE : AIRTON LANGARO DIPP
IDENTIDADE : 2.005.603.432-SSP/RS
CPF. : 122.776.730-72

DIRETOR DE TECNOLOGIA E INFRA-ESTRURA: EDUARDO MEDEIROS DE MORAIS
IDENTIDADE : 453.609 SSP/DF
CPF. : 150.199.771-87

CONTRATADA: HEWLETT-PACKARD BRASIL LTDA
CNPJ.: 61.797.924/0001-55
INSCRIÇÃO ESTADUAL: 206.203.572.117
ENDEREÇO: AL. RIO NEGRO, 750 – ALPHAVILLE – BARUERI/SP
CEP: 06454-000
TELEFONE: (11) 4197-8000
FAX: (11) 4197-8432

DEPARTAMENTO JURÍDICO
E C T
03 OUT 2003
Contrato nº 12104
BRASÍLIA - DF

REPRESENTANTES

DIRETOR : IVO ROMANI
IDENTIDADE: 7.187.356-9 SSP/SP
CPF.: 903.621.798-91

REPRESENTANTE DE VENDAS: JOSÉ EDUARDO PIRES DO RIO RIBEIRO
IDENTIDADE: 15.319.247 SSP/SP
CPF.....: 071.885.858-14

(61) 329-6055

DEPARTAMENTO JURÍDICO E C T
Conforme MJ/DEJUR/DJTEC MAC 70775

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls: 0989
Doc: 3685

CLÁUSULA PRIMEIRA - DO OBJETO

1.1. O presente Termo Aditivo tem por objeto o acréscimo de 13,46 % (treze vírgula quarenta e seis por cento) do valor global do Contrato nº 11.994/2003, para prestação de serviços de locação e instalação de **119 (cento e dezenove) servidores Intel Tipo 03**, novos de fábrica, incluindo a configuração, assistência técnica e garantia, conforme quantidades, locais de entrega e modelos descritos no **Anexo I** deste Termo Aditivo.

CLÁUSULA SEGUNDA – DO CRONOGRAMA DE EXECUÇÃO

2.1. A Contratada deverá obedecer o seguinte cronograma de execução :

Fase	Descrição	Prazo(dias)
I	Entrega, Instalação e Configuração dos Equipamentos em até	D + 90
II	Aceitação Final dos Equipamentos em até	D + 120

(Onde D = Data de Assinatura deste Instrumento) :

mensal 2.499,86 × 48 =
unitário 119.996,28 × 119 =
14.279.200,32
2.499,86 × 48m
119.993,28 48m

CLÁUSULA TERCEIRA – DO PREÇO E PAGAMENTO

3.1. O preço de locação mensal é, por servidor locado, R$ 2.499,86 (dois mil quatrocentos e noventa e nove reais e oitenta e seis centavos), totalizando R$ 119.993,28 (cento e dezenove mil novecentos e noventa e três reais e vinte e oito centavos) para 48 meses.

3.2. Os pagamentos serão efetuados mediante a apresentação de Nota(s) Fiscal(is)/Fatura(s) para cada uma das Diretorias Regionais descritas no **Anexo I,** devidamente atestada(s) pela **CONTRATANTE**, mensalmente durante os **48(quarenta e oito)** meses de alugueres, no **15º (décimo quinto) dia** do mês subseqüente ao da prestação dos serviços , após a emissão do **Termo de Aceitação da Fase II** acima.

CLÁUSULA QUARTA – DA GARANTIA DE EXECUÇÃO

4.1. A **CONTRATADA** comprovará no prazo de **05 (cinco) dias úteis** da data de assinatura deste Termo Aditivo, a efetivação da garantia de execução contratual, que deverá corresponder à vigência do presente Instrumento, em percentual equivalente a **3%(três por cento)** do valor da alteração, correspondente a **R$ 428.376,00** (quatrocentos e vinte e oito mil trezentos e setenta e seis reais) , podendo optar por uma das seguintes modalidades :

DEPARTAMENTO JURÍDICO
Conforme
NJ/DEJUR/DJTEC
RQS nº 03/2005 - CN - CPMI - CORREIOS
Mat. 70775
Fls: 0990
Doc: 3685

a) caução em dinheiro ou títulos da dívida pública;
b) seguro-garantia;
c) fiança bancária.

4.2. Em caso de garantia em dinheiro, a **CONTRATADA** deverá depositar o valor em nome da **CONTRATANTE** , conforme dados abaixo :

BANCO: Banco do Brasil S.A. (001)
AGÊNCIA: 3307-3
CONTA CORRENTE: 195.159-9

CLÁUSULA QUINTA – DO VALOR DA ALTERAÇÃO

5.1. O aditamento em questão implicará em acréscimo de R$ 14.279.200,32 (quatorze milhões duzentos e setenta e nove mil duzentos reais e trinta e dois centavos) no valor global do Contrato nº 11.994/2003.

CLÁUSULA SEXTA - DO VALOR GLOBAL

6.1 O valor global do Contrato nº 11.994/2003, acrescido do valor deste aditivo, passará a ser de R$ 120.316.069,51 (cento e vinte milhões trezentos e dezesseis mil sessenta e nove reais e cinqüenta e um centavos).

CLÁUSULA SÉTIMA – DOS RECURSOS ORÇAMENTÁRIOS

7.1. As despesas decorrentes da prestação de serviços, objeto deste aditamento, correrão por conta da seguinte classificação orçamentária :

Conta: 800.07.03.0000 Atividade: 00.8.00

CLÁUSULA OITAVA – DA VIGÊNCIA

8.1. O presente Termo Aditivo vigorará a partir da data de sua assinatura até o limite da vigência do Contrato no. 11.994/2003.

DEPARTAMENTO JURÍDICO DECT
Conforme MJ/DEJUR/DJTEC
RQS nº 03/2005 - CN - CPMI - CORREIOS
Mat. 76773
Fls: 0991
3685
Doc:

CLÁUSULA NONA – DA FUNDAMENTAÇÃO LEGAL E DA AUTORIZAÇÃO

9.1. O presente Termo Aditivo tem respaldo legal no subitem 2.11 da Cláusula Segunda e no subitem 7.1.1, alinea "b" da Cláusula Sétima do Contrato nº 11.994/2003 e na Lei nº 8.666/93, Artigo 65, Inciso I, Alínea "b" e Parágrafo 1º.

CLÁUSULA DÉCIMA – DA RATIFICAÇÃO

10.1. Ficam ratificadas as demais cláusulas e condições do Contrato Original, que não conflitem com as alterações ora acordadas.

E, por estarem justas e acordadas, as partes assinam o presente Termo Aditivo em **02 (duas) vias** de igual teor e forma e para um só efeito, na presença das testemunhas abaixo assinadas.

Brasília/DF, 03 de outubro de 2003.

PELA CONTRATANTE:

AIRTON LANGARO DIPP
Presidente

EDUARDO MEDEIROS DE MORAIS
Diretor de Tecnologia e Infra-Estrutura

PELA CONTRATADA:

IVO ROMANI
Diretor

JOSÉ EDUARDO PIRES DO RIO RIBEIRO
Representante de Vendas

TESTEMUNHAS:

1. _____
CPF: 488 866 530 34

2. _____
CPF: 115.805.931-00

DEPARTAMENTO JURÍDICO
Conforme NJ/DEJUR/DJTEC

RQS nº 03/2005 - CN - CPMI - CORREIOS
MAC 70775
Fls: 0992
3685
Doc:

PAUTA DE DISTRIBUIÇÃO DOS EQUIPAMENTOS

1. PAUTA DE DISTRIBUIÇÃO

SEQ	LOCALIDADE	SERVIDOR INTEL TIPO 03 BD	SERVIDOR INTEL TIPO 03 BK
1	AC	1	1
2	AL	2	1
3	AM	2	1
4	BA	5	2
5	BSB	3	2
6	CE	3	1
7	ES	4	1
8	GT	3	1
9	MA	5	1
10	MG	6	2
11	MS	3	1
12	MT	3	1
13	NO	2	1
14	PA	2	1
15	PB	2	1
16	PE	3	1
17	PI	2	1
18	PR	5	2
19	RJ	6	1
20	RN	2	1
21	RS	6	2
22	SC	4	2
23	SE	2	1
24	SPI	4	2
25	SPM	8	0
TOTAL POR TIPO		88	31
TOTAL GERAL		119	

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls: 0993
3685
Doc:

DEPARTAMENTO JURÍDICO
Conforme
MJ/DEJUR/DJTEC

1.1 ENDEREÇOS PARA ENTREGA E MANUTENÇÃO DOS EQUIPAMENTOS

DIRETORIA REGIONAL	RESPONSÁVEL	ENDEREÇO	TELEFONES DIRETOS
AC	WALDIMIR/JEFFERSON	SBN – Quadra 01 – Conj 03 – Bl. A – Ed. Sede ECT – 2º SS 70002 – 900 – Brasília/DF	61-426.2214/1754 Fax: 426.2206
AL	JOÃO BATISTA/PLISTHEUS	Rua do Sol, 57 – Centro 57020-900 – Maceió/AL	82-216.7006/7057 Fax: 216.7110
AM	ALVES/ELDON	Av. André Araújo, 82 – Bairro Aleixo 69060-970 - Manaus/AM	92-611.1454/663.5846 Fax: 611.4892
BA	INALDO	Av. Paulo VI, 190 – 6º Andar - Pituba 41810-900 – Salvador/BA	71-346.2600/2602 Fax: 346.2601
BSB	MÁRIO ÂNGELO CHERIN/FRANCISCO	SESPS 712/912 – Bloco III – Conj. PASTEUR – 1º Andar – Asa Sul 70390-125 – Brasília/DF	61-345.3012/2999 Fax: 345.3456
CE	HENRIQUE/REZENDE	Rua Senador Alencar, 38 – 2º Andar – Sala 212 – Centro 60030-050 – Fortaleza/CE	85-255.7180/85/86/89 Fax: 255.7188
ES	ROBSON/ALAERTE	Av. Leitão da Silva, 2730 – Santa Luiza 29045-902 – Vitória/ES	27-3334.3235 Fax: 3334.3280
GT	EUGÊNIO/PAULO	Praça Dr. Pedro Ludovico Teixeira, 11 2º And. Centro – 74002-900 – Goiânia/GO	62-226.2027 Fax: 226.2043
MA	ANTÔNIO JORGE/	BR 135 – KM 0 – Tiriricau 65095-971 – São Luiz/MA	Fone/Fax: 98-244.5491
MG	LÚCIO/DARCY	Av. Afonso Pena, 1270 – 1º and. – Centro 30130-900 – Belo Horizonte/MG	31-3249.2158 Fax: 3243.2206
MS	ONÉSIMO ROMEU/JOARÍ	Rua Vasconcelos Fernandes, 164 79008/970 – Campo Grande/MS	67-389.5113 Fax: 389.5262
MT	LAIR/JORGE	Av. Dom Orlando Chaves, 1087 78005-900 – Cuiabá/MT	65-688.1120 Fax: 688.1124
NO	JOSÉ ANTÔNIO/ANGELO	Av. Costa e Silva, 2137 – São Sebastião I 78904-050 - Porto Velho/RO	69-216.2514 Fax: 216.2526
PA	MARCELO/FERNANDO PANTOJA	Av. Presidente Vargas, 498 – Centro 66017-970 – Belém/PA	91-211.3005 Fax: 211.3035
PB	EDNALDO/JAIR	BR 230 – KM 24- Cristo Redentor 58002-900 – João Pessoa/PB	83-216.3528 Fax: 216.3528
PE	SORAIA/BEZERRIL	Av. Guararapes, 250 -- 3º andar – Centro 51010-900 – Recife/PE	81-425.3751 Fax: 425.3749
PI	BENEDITO/CHRISTIANE	Av. Antonino Freire,1407 – Centro 64001-040 – Teresina/PI	86-215.3550 Fax: 215.3593
PR	JOSÉ ADEMIR	R. João Negrão, 1251 – Bl. 02 – 2º andar Rebouças – 80002-900 – Curitiba/PR	41-310.2086 Fax: 310.2098
RJ	RICARDO RIVAS/JAIME GUERRA	Av. Presidente Vargas, 3.077 – 6º andar 20202-900 – Rio de janeiro/RJ	21-2503.8381/82 Fax: 2503.8348
RN	ARTUR/LICURGO	Av. Eng.º Hidelbrando de Góis, 221 Ribeira – 59002-900 – Natal/RN	84-220.2440/41 Fax: 220.2441
RS	SILVIO/ROBERTO EICK	Av. Siqueira Campos, 1100 – 3º andar 90002-900 – Porto Alegre/RS	51-3220.8809 Fax: 3220.8815
SC	VÂNIA	Praça 15 de novembro, 242 Florianópolis/SC	48-229.4315 Fax: 223.7996
SE	ROBERTO ALMEIDA	Rua Acre, 1089 – Siqueira Campos 49000-075 - Aracaju/SE	79-241.4315 Fax: 241.4315
SPM	MAURO/SÔNIA	Rua Mergenthaler, 592 – Bl. 2 – Vila Leopoldina – 05311-900 – São Paulo/SP	11-3838.7700 Fax: 3838.7702
SPI	LUIS DE SÁ/JAIR	Praça Dom Pedro II, 455 – 3º andar 17015-905 – Bauru/SP	14-238.3622 Fax: 226.1599

ESPECIFICAÇÕES TÉCNICAS DOS EQUIPAMENTOS

REQUISITOS ESSENCIAIS AOS EQUIPAMENTOS (OBRIGATÓRIOS)

2. ASPECTOS GERAIS

Os itens descritos a seguir são obrigatórios e deverão ser observados para todos os produtos que compõem a proposta técnica.

REQUISITO	DESCRIÇÃO
1 – Comprovação de PERFORMANCE	a. Todos os equipamentos da plataforma **INTEL** para os quais for solicitado valor de performance baseado em **tpm-C**, deverão apresentar a comprovação por documentação adequada do valor de **tpm-C** auditado pelo **Transaction Processing Performance Council – TPC (www.tpc.org)** para o equipamento cotado ou para equipamento da mesma arquitetura do cotado. Entende-se por equipamento da mesma arquitetura, equipamento do mesmo fabricante, com o mesmo tipo e quantidade de processadores e com clock igual ou superior ao equipamento cotado. b. Caso o equipamento cotado não tenha sido ainda auditado com o número de processadores proposto, deverá ser informado um cálculo estimado, desde que o valor utilizado como referência para a estimativa de **tpm-C** tenha sido obtido em equipamento auditado do mesmo fabricante, com o mesmo tipo e quantidade de processadores e com clock igual ou inferior ao equipamento cotado; c. No caso de performance estimada, a mesma deverá ser calculada com base na fórmula: **tpm-C estimado = tpm-C auditado * (NCPU_O * CLOCK_O / NCPU_A * CLOCK_A)** Onde: **NCPU_O**: Número de CPU da Configuração Ofertada **CLOCK_O**: Clock da CPU Ofertada **NCPU_A**: Número de CPU da Configuração Auditada pelo TPC **CLOCK_A**: Clock da CPU Auditada pelo TPC
2 – Requisitos Gerais	d. Os equipamentos deverão ser novos de fábrica e entregues acondicionados adequadamente em caixas fechadas, de forma a permitir completa segurança durante o transporte; e. Deverão ser fornecidos pela **CONTRATADA**, quando da entrega e instalação dos produtos, todos os cabos, acessórios, manuais e documentações completas, que são necessários ao pleno funcionamento dos equipamentos, softwares e periféricos; f. Serão consideradas para efeitos das quantidades mínimas exigidas, apenas **1 (uma)** placa/controladora de rede instalada **"ON BOARD"** na placa de sistema.
3 – Garantia	g. É de total responsabilidade da **CONTRATADA**, pelo período de **48 (quarenta e oito) meses** a partir da data do aceite final dos equipamentos.

4 – Compatibilidade	h. Todos os componentes de hardware dos **Servidores INTEL** fornecidos, deverão estar constantes na **HCL (Hardware Compatibility List)** da Microsoft como compatíveis com o Sistema Operacional Windows 2000 Server, Advanced Server ou posterior equivalente na categoria "CLUSTER" e na categoria "SYSTEM/SERVER MULTIPROCESSOR"; i. Todos os componentes de hardware dos **Servidores INTEL** fornecidos deverão funcionar **EM CONJUNTO**, simultaneamente e sem conflitos.
5 – Assistência Técnica	j. A **CONTRATADA** deverá prestar os serviços de assistência técnica nos locais de instalação dos equipamentos (assistência ON-SITE); k. Os serviços prestados deverão englobar a substituição de peças e componentes defeituosos dos equipamentos, bem como a depuração e resolução de problemas relacionados ao ambiente de software fornecido pela **CONTRATADA.**
6 – Recursos Mínimos de Gerenciamento do Hardware	l. Os equipamentos **SERVIDORES INTEL** ofertados, deverão prover mecanismos de detecção de pré-falha dos seguintes componentes vitais ao sistema: **CPU, MEMÓRIA RAM E DISCOS INTERNOS;** m. A **CONTRATADA** deverá fornecer **TODOS OS COMPONENTES DE SOFTWARE** necessários a montagem de uma estrutura de gerência de pré-falhas, tais como: agentes, frameworks, consoles ou quaisquer componentes de software necessários ao pleno funcionamento desta gerência; n. Deverão ser fornecidas todas as licenças necessárias para todos os equipamentos em cada localidade de instalação.
7 – Comprovação dos Requisitos Técnicos	o. No fornecimento da documentação técnica, é exigido que sejam fornecidos obrigatoriamente todos os informes, conforme descritos nos subitens que seguem: p. A documentação que acompanha o equipamento deve ser em língua portuguesa, espanhola ou inglesa, preferencialmente em língua portuguesa; q. A identificação do Fabricante, da Marca e do Modelo do produto. r. Comprovação de todos os atributos técnicos exigidos nesta planilha de especificações técnicas, atestada pelo fornecimento do descrito em qualquer dos subitens que seguem ou pelo conjunto destes: s. Prospecto técnico do modelo cotado, o qual deve ser preferencialmente no original ou fotocópia legível e completa, com grifo nas características técnicas a serem informadas; t. Cópia legível e atual da página Internet do Fabricante onde constem às especificações técnicas do modelo do produto cotado, com grifo nas características técnicas a serem informadas.
8 – Atualizações dos Softwares Embarcados nos Equipamentos	u. A **CONTRATADA** deverá entregar, sem ônus para a **CONTRATANTE**, as mídias com todas as atualizações dos softwares enbarcados fornecidos nos equipamentos, tais como e não se limitando a: atualizações de firmware, BIOS, microcódigo etc, durante a **VIGÊNCIA DO CONTRATO**; v. A **CONTRATADA** deverá entregar cópia de todas as atualizações em cada localidade de instalação dos equipamentos.

3. ESPECIFICAÇÕES TÉCNICAS DOS EQUIPAMENTOS

3.1 SERVIDOR INTEL TIPO 03 BD – SERVIDOR DE BANCO DE DADOS

ATRIBUTO	CONFIGURAÇÃO MÍNIMA EXIGIDA PARA CADA EQUIPAMENTO
1 - Descrição	a. Servidor composto por processadores **INTEL**, com no mínimo **2 (dois)** processadores **INTEL XEON**, com clock mínimo de **2,8 GHz**; b. O equipamento deverá apresentar performance mínima de **34.000 tpm-C**, conforme especificado no **Subitem 1.1.**;. c. Os equipamentos deverão ser montados em RACKS de 19" de acordo com o **Subitem 2.6.**, a serem fornecidos pela **CONTRATADA.**
2 - Barramento	d. Barramento do sistema de, no mínimo, 533 MHz.
3 - Memória Cache L2	e. 512KByte por processador.
4 - Memória RAM	f. 4GB (quatro gigabytes) ECC SDRAM ou tecnologia superior, instalada.
5 - Controladora e Unidade de Disco Rígido - Interno	g. No mínimo, **5 (cinco) discos** com capacidade nominal mínima de **73 GB (setenta e três gigabytes)** montados em arranjo **RAID 5**, por hardware; h. A controladora RAID deverá possuir o mínimo de **64 MB (sessenta e quatro megabytes)** de memória cache, por canal. i. Os discos deverão possuir tempo médio de acesso menor ou igual a 6 ms, padrão SCSI, funcionalidade "HOT SWAP", com velocidade de rotação mínima de 10.000 RPM; j. As controladoras deverão ser padrão Wide Ultra 3 SCSI ou superior e funcionalidade "HOT SWAP" para os discos; k. Adicionalmente, deverá ser disponibilizado internamente no gabinete de discos, **1 (um) disco** com capacidade nominal mínima de **73 GB (setenta e três gigabytes)** para implementar a funcionalidade de **"HOT-SPARE"**. Este disco deverá seguir os padrões descritos nos itens anteriores.
6 - Interface de VIDEO	l. Padrão SVGA, PCI 32 Bits ou superior, com 8 Mbytes no mínimo.
7 - Unidade de CD-ROM	m. Uma unidade interna, tecnologia IDE ou SCSI, com velocidade mínima de 24X.
8 - Controladora de I/O (por equipamento)	n. Deverão ser disponibilizadas 2 (duas) interfaces de rede Fast Ethernet – IEEE 802.3, saídas 100BaseTX com possibilidade de gerenciamento SNMP.
9 - Ambiente Operacional	o. Os servidores deverão ser fornecidos com o sistema operacional Microsoft Windows Server 2003 Standard Edition, instalado e licenciado.
10 - Fonte de Alimentação	p. Fontes instaladas na capacidade máxima do equipamento, com recurso de troca sem interrupção, funcionalidade "HOT-SWAPPABLE", e alimentação elétrica de 110 e 220 Volts, com comutação automática ou manual e freqüência de operação de 60 (sessenta) Hertz; q. As fontes de alimentação deverão ser redundantes por fontes internas independentes, cada fonte de alimentação deverá prover alimentação própria, de tal forma que, em caso de falha de uma das fontes ou cabo de alimentação o equipamento continue a funcionar sem prejuízo da sua disponibilidade.

11 - Unidade de Backup	r. 1 (uma) unidade leitora/gravadora padrão DDS 3 ou superior, interna ao servidor; s. No fornecimento deve-se prever a entrega de 2 (duas) fitas novas e 1 (uma) fita para limpeza.

3.2 SERVIDORES INTEL TIPO 03 BK – SERVIDOR DE BACKUP

ATRIBUTO	CONFIGURAÇÃO MÍNIMA EXIGIDA PARA CADA EQUIPAMENTO
1 - Descrição	a. Servidor composto por processadores **INTEL**, com no mínimo **1 (um)** processador **INTEL XEON**, com clock mínimo de **3,06 GHz**; b. O servidor deverá ser expansível a, no mínimo, **2 (dois)** processadores; c. Os equipamentos deverão ser montados em RACKS de 19" de acordo com o **Subitem 2.6.**, a serem fornecidos pela **CONTRATADA**.
2 - Barramento	d. Barramento do sistema de, no mínimo, 533 MHz.
3 - Memória Cache L2	e. 512KByte por processador.
4 - Memória RAM	f. 2GB (dois gigabytes) ECC SDRAM ou tecnologia superior, instalada.
5 - Controladora e Unidade de Disco Rígido - Interno	g. No mínimo, **5 (cinco) discos** com capacidade nominal mínima de **73 GB (setenta e três gigabytes)** montados em arranjo **RAID 5**, por hardware; h. A controladora RAID deverá possuir o mínimo de **64 MB (sessenta e quatro megabytes)** de memória cache, por canal. i. Os discos deverão possuir tempo médio de acesso menor ou igual a 6 ms, padrão SCSI, funcionalidade "HOT SWAP", com velocidade de rotação mínima de 10.000 RPM; j. As controladoras deverão ser padrão Wide Ultra 3 SCSI ou superior e funcionalidade "HOT SWAP" para os discos; k. Adicionalmente, deverá ser disponibilizado internamente no gabinete de discos, **1 (um) disco** com capacidade nominal mínima de **73 GB (setenta e três gigabytes)** para implementar a funcionalidade de **"HOT-SPARE"**. Este disco deverá seguir os padrões descritos nos itens anteriores.
6 - Interface de VIDEO	l. Padrão SVGA, PCI 32 Bits ou superior, com 8 Mbytes no mínimo.
7 - Unidade de CD-ROM	m. Uma unidade interna, tecnologia IDE ou SCSI, com velocidade mínima de 24X.
8 - Controladora de I/O (por equipamento)	n. Deverão ser disponibilizadas 2 (duas) interfaces de rede Fast Ethernet – IEEE 802.3, saídas 100BaseTX com possibilidade de gerenciamento SNMP.
9 - Ambiente Operacional	o. Os servidores deverão ser fornecidos com o sistema operacional Microsoft Windows Server 2003 Standard Edition, instalado e licenciado; p. Deverão ser fornecidos, para todos os servidores **INTEL Tipo 02**, software de controle e gerência de backup e restore, na versão **SERVIDOR**, com suas respectivas licenças de uso; q. Deverão ser fornecidos, para todos os servidores do **ANEXO 1-A**, com exceção dos servidores **INTEL Tipo 02**, software de controle e gerência de backup e restore, na versão **CLIENTE**, com suas respectivas licenças de uso;

9 - Ambiente Operacional (continuação)	r. Os softwares, na versão **SERVIDOR**, deverão possuir as seguintes características mínimas: s. Deverá gerenciar e permitir as operações automáticas de backup e restore utilizando a **UNIDADE AUTOLOADER** especificada no **subitem 2.2.11.**, devendo ser totalmente compatível com a mesma; t. Realizar o backup e restore full, incremental e diferencial para todos os servidores especificados no **ANEXO 1-A**; u. Permitir o backup de arquivos abertos "FLAT FILES" para todos os servidores especificados no **ANEXO 1-A**; v. Possibilitar que o agendamento de backups seja feito por data específica, diário, semanal ou mensal; w. Permitir a restauração parcial de dados de backups, recuperando versões anteriores de arquivos e diretórios individuais sem a necessidade de restauração de toda uma imagem de backup; x. Possuir capacidade de restore independente do servidor onde tenha sido feito o backup; y. Realizar alocação automática de fitas na **UNIDADE AUTOLOADER**; z. Possuir ambiente gráfico de gerenciamento de backup e restore, que deve permitir configuração e monitoração centralizada a partir de uma console única; aa. Possuir gerenciamento gráfico on-line da situação dos backups realizados e sua restauração.
10 - Fonte de Alimentação	bb. Fontes instaladas na capacidade máxima do equipamento, com recurso de troca sem interrupção , funcionalidade "HOT-SWAPPABLE", e alimentação elétrica de 110 e 220 Volts, com comutação automática ou manual e freqüência de operação de 60 (sessenta) Hertz; cc. As fontes de alimentação deverão ser redundantes por fontes internas independentes, cada fonte de alimentação deverá prover alimentação própria, de tal forma que, em caso de falha de uma das fontes ou cabo de alimentação o equipamento continue a funcionar sem prejuízo da sua disponibilidade.
11 - Unidade Autoloader	dd. Deverá ser fornecida **1** (uma) **UNIDADE AUTOLOADER,** com capacidade de armazenar pelo menos 7 (sete) cartuchos LTO Ultrium 2; ee. A **UNIDADE AUTOLOADER** deverá possuir sistema automático de troca de cartuchos, sem a interferência do usuário; ff. A unidade deverá possuir **1 DRIVE** de leitura e gravação, **PADRÃO LTO ULTRIUM 2**, com capacidade de realizar transferência à pelo menos 30 MBytes/s; gg. A **UNIDADE AUTOLOADER** deverá possuir interface SCSI Ultra2 ou superior, cabo e controladora SCSI para ser conectada ao **SERVIDOR INTEL TIPO 02**; hh. Deverão ser fornecidos, para cada **UNIDADE AUTOLOADER**, 7 (sete) cartuchos LTO Ultrium 2, com capacidade nativa de 200GB; ii. A **UNIDADE AUTOLOADER** deverá possuir gabinete do tipo rack-mountable com altura máxima de 4U; jj. A **UNIDADE AUTOLOADER** deverá ser montada em **RACK** de 19" de acordo com o **Subitem 2.6.**

DEPARTAMENTO JURÍDICO

Conforme
MJ/DEJUR/DJTEC

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls: 0999

Doc: 3685

3.3 COMUTAÇÃO DE VÍDEO, MOUSE E TECLADO

ATRIBUTO	CONFIGURAÇÃO MÍNIMA EXIGIDA POR EQUIPAMENTO
1 – Descrição	a. Deverá ser fornecido pela **CONTRATADA**, para cada localidade de instalação dos servidores, equipamentos para comutação de teclado, vídeo e mouse, devendo atender a todos os servidores fornecidos para aquela localidade, incluindo possíveis servidores legados da **CONTRATANTE** existentes nas localidades de instalação; b. Os equipamentos deverão ser montados em RACKS de 19" de acordo com o **Subitem 2.6.**, a serem fornecidos pela **CONTRATADA**; c. Será permitida, para os servidores da Plataforma INTEL, fornecidos pela **CONTRATADA**, a utilização de Hardware para Gerenciamento Remoto, em substituição aos equipamentos especificados acima, desde que as características deste hardware, descritas no **Subitem 2.5.4.** deste **ANEXO** sejam atendidas.
2 – Quantidade de Portas	d. O conjunto de equipamentos fornecidos para cada localidade deverá disponibilizar um mínimo de **16 (dezesseis)** portas de comutação.
3 – Consoles	e. Deverá ser disponibilizado, em cada localidade, um conjunto de 2 (duas) consoles para acesso remoto aos servidores conectados nos comutadores de teclado, vídeo e mouse; f. As consoles devem ser independentes entre si, podendo acessar qualquer servidor, inclusive os servidores legados descritos no **Subitem 2.5.1.**; g. As consoles deverão utilizar monitores de vídeo que alcancem resolução de 1280x1024 60Hz com no mínimo com 17" (dezessete polegadas), policromático e DOT PITCH 0,28, mouse e teclado padrão ABNT2; h. As consoles poderão ser montadas a uma distância de aproximadamente 30 (trinta) metros. Todos os materiais e componentes necessários a esta montagem deverão ser fornecidos pela **CONTRATADA**.

4 – Solução Alternativa para comutação dos Servidores INTEL	i. A **CONTRATADA** poderá substituir portas de comutação de teclado, vídeo e mouse por controladoras que permitam o Gerenciamento Remoto, para os servidores da plataforma INTEL fornecidos, de forma que 1 (uma) controladora de gerenciamento remoto substitui 1 (uma) porta de comutação solicitada; j. O Hardware para Gerenciamento Remoto deverá possuir as seguintes características técnicas: o Placa PCI instalada em slot do mesmo padrão ou integrada a placa – mãe; o Deve funcionar independentemente do Sistema Operacional; o Deve permitir o acompanhamento e controle de todo o ciclo de inicialização do servidor, incluindo as etapas de POST (Power On Self Test) e carga do Sistema Operacional; o Deve ser do mesmo fabricante do servidor; o Deve possibilitar a utilização de console remota gráfica através de browser; o Deve implementar mecanismo de segurança para a comunicação entre o browser e o dispositivo de gerenciamento, através utilização do padrão SSL (Security Socket Layer) 128 bits; o Deve possuir interface Ethernet 10/100 Mbits ou superior dedicada, suportando alocação fixa de endereço IP; o Possibilidade de ligar/desligar o servidor remotamente, para usuários autenticados; o Deve implementar mecanismo de autenticação para usuários no próprio dispositivo de gerenciamento.
5 – Gerais	k. Deverão ser fornecidos todos os cabos e acessórios necessários para conectar servidores legados nas demais portas disponíveis, após a conexão dos servidores fornecidos; l. Os cabos de interligação dos equipamentos fornecidos ao comutador deverão ter comprimento mínimo de 6 (seis) metros. Nas localidades onde sobrarem portas de comutação, os cabos adicionais deverão ter comprimento mínimo de 30 (trinta) metros; m. Os cabos de interligação das consoles aos equipamentos de comutação deverão ter comprimento mínimo de 30 (trinta) metros; n. A escolha do servidor a ser comutado deve ser feita por menu configurável, utilizando os nomes dos servidores designados pela **CONTRATANTE**; o. Todos os equipamentos utilizados para a comutação deverão possuir alimentação elétrica de 90 a 240 volts com comutação automática ou manual e freqüência de operação de 60 (sessenta) Hertz.

3.4 RACK PARA EQUIPAMENTOS

ATRIBUTO	CONFIGURAÇÃO MÍNIMA EXIGIDA PARA CADA EQUIPAMENTO
1 – Estrutura Física	a. Todos os equipamentos fornecidos, deverão ser instalados em Estruturas de **RACK**, com as seguintes características: o **RACK** do tipo fechado, em alumínio ou aço, com 19" de largura e profundidade de, no mínimo, 77cm, para fixação dos equipamentos fornecidos; o Altura mínima de 40Us; o Deverá permitir a instalação de todos os equipamentos com largura padrão de 19" (dezenove polegadas); o ventilação; o colunas de segundo plano (aproximadamente 10 cm); o sistema de chave e fechadura; laterais e traseiras removíveis.
2 – Estrutura Funcional	b. Os racks deverão ser interligados à rede elétrica através de tomadas tripolares, a serem fornecidas juntamente com o **RACK** pela **CONTRATADA**; c. A **CONTRATADA** fornecerá e instalará réguas com tomadas em número suficiente para todos os servidores e equipamentos instalados no interior do **RACK**. A pinagem da régua deverá ser compatível com o padrão das tomadas dos equipamentos a serem conectados.
3 – Gerais	d. Deverá ser fornecido pelo menos 1 (um) **RACK** por localidade onde serão instalados os equipamentos.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls: 1002
3685
Doc:

DEPARTAMENTO JURÍDICO
Conforme
NJ/DEJUR/BJTEC

CONTRATO DE PRESTAÇÃO DE SERVIÇOS DE LOCAÇÃO DE EQUIPAMENTOS DE INFORMÁTICA, INCLUINDO ASSISTÊNCIA TÉCNICA E TREINAMENTO DE PESSOAL

CONTRATANTE: EMPRESA BRASILEIRA DE CORREIOS E TELÉGRAFOS

CNPJ : 34.028.316/0001-03
INSCRIÇÃO ESTADUAL: 07.333.821/002-05
ENDEREÇO: SBN Quadra 01 Conjunto 03 Bloco A – 6º Andar – Ed. Sede/ECT
CEP: 70.002-900 – Brasília/DF

DEPARTAMENTO JURÍDICO
E C T
12 AGO 2003
Contrato nº 1094
BRASÍLIA - DF

REPRESENTANTES:

PRESIDENTE: AIRTON LANGARO DIPP
DOCUMENTO DE IDENTIDADE: 2.005.603.432 – SSP/RS
CPF: 122.776.730-72

DIRETOR DE TECNOLOGIA E DE INFRA-ESTRUTURA: EDUARDO MEDEIROS DE MORAIS
DOCUMENTO DE IDENTIDADE: 453.609 – SSP/DF
CPF: 150.199.771-87

CONTRATADA: HEWLETT-PACKARD BRASIL LTDA
CNPJ : 61.797.924/0001-55
INSCRIÇÃO ESTADUAL: 206.203.572.117
ENDEREÇO: AL. RIO NEGRO, 750 – ALPHAVILLE – BARUERI/SP
CEP: 06454-000
TELEFONE: (11) 4197-8000
FAX : (11) 4197-8432

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls: 1003
3685
Doc:

REPRESENTANTES:

DIRETOR: IVO ROMANI
DOCUMENTO DE IDENTIDADE: 7.187.356-9 – SSP/SP
CPF: 903.621.798-91

REPRESENTANTE DE VENDAS: JOSÉ EDUARDO PIRES DO RIO RIBEIRO
DOCUMENTO DE IDENTIDADE: 15.319.247 - SSP/SP
CPF: 071.885.858-14

DEPARTAMENTO JURÍDICO E C T
Conforme
NJ/DEJUR/DJTEC

CLÁUSULA PRIMEIRA - DO OBJETO

1.1. O presente Contrato tem como objeto a prestação de serviços de locação e instalação de **162 (cento e sessenta e dois)** equipamentos de informática – novos de fábrica - incluindo **a configuração, o treinamento, a assistência técnica e a garantia**, destinados aos Centros Corporativos de Dados da ECT, localizados nas cidades de Brasília e São Paulo, conforme as condições específicas, pauta de distribuição e as especificações constantes dos **ANEXOS 1-A e 1-B** deste Contrato.

CLÁUSULA SEGUNDA - DAS OBRIGAÇÕES DA CONTRATADA

2.1. Caberá à **CONTRATADA** locar, garantir compatibilidade e portabilidade, conforme **Item 1.6** do **ANEXO 1-A** deste Contrato, instalar, configurar, dar garantia e assistência técnica aos equipamentos locados e realizar os treinamentos, durante a vigência da locação;

2.1.1. A locação deverá contemplar, no mínimo, os **PRODUTOS** descritos nos **ANEXOS 1-A** e **1-B** deste Contrato, provendo a:

a) Preparação do ambiente de produção, realizando integração e interoperabilidade com o ambiente já existente, relativamente aos itens: Rede TCP/IP e Segurança de Rede;

b) Integração e interoperabilidade da Rede SAN – Storage Area Network, existente na **CONTRATANTE** à Rede SAN fornecida, de forma que os Servidores e os Sistemas de Backup fornecidos pela **CONTRATADA** possam acessar os dados armazenados no atual sistema de armazenamento (Storage IBM 2105 F20), com a performance compatível com as aplicações existentes.

2.2. A **CONTRATADA** deverá apresentar, para validação da **CONTRATANTE**, em até **45 (quarenta e cinco) dias** após a assinatura deste Contrato, cronograma de trabalho, conforme descrito no **ANEXO 1-A** deste Termo.

2.3. A **CONTRATADA** deverá obedecer o seguinte cronograma de execução:

Fase	Descrição	Prazo (dias)
I	**Apresentação do Cronograma de Trabalho em até**	**D + 45**
II	**Entrega, Instalação e Configuração dos Equipamentos em até**	**D + 90**
III	**Aceitação Final dos Equipamentos em até**	**D + 120**
IV	**Treinamento Operacional em até**	**FIII + 30**
V	**Treinamento Oficial em até**	**FIII + 720**
VI	**Treinamento On-Site em até**	**FIII + 1440**

Onde: **D = Data de Assinatura do Contrato.**
FIII = Data de Emissão do Termo de Aceite da Fase III.

RQS nº 03/2005 - CN - CPMT - CORREIOS
1004
Fls:
3685
Doc:

DEPARTAMENTO JURÍDICO E C T
Conforme
NJ/DEJUR/DJTEC ____/____

2.4. Caberá à **CONTRATADA**, se necessário for, o ônus pela instalação dos recursos necessários para o perfeito funcionamento dos equipamentos locados, onde deverão ser observados os requisitos de qualidade e segurança adotados pela **CONTRATANTE**, conforme descrito no **ANEXO 1-A** deste Contrato.

2.4.1. Se forem instalados quaisquer recursos de suporte aos equipamentos locados, os mesmos não farão parte da locação e deverão permanecer com a **CONTRATANTE** após o término do Contrato.

2.5. A **CONTRATADA** deverá proceder a entrega e a instalação física de todos os equipamentos nas Salas de Segurança Física, situadas na Administração Central – AC, em Brasília-DF e na Diretoria Regional de São Paulo Metropolitana - DR/SPM, em São Paulo/Capital, conforme a pauta de distribuição e as condições constante dos **ANEXOS 1-A e 1-B** deste Contrato.

2.5.1. Serão de exclusiva responsabilidade da **CONTRATADA** a entrega, a instalação, a configuração, os testes, e a assistência técnica dos **PRODUTOS** bem como o fornecimento dos recursos adicionais que sejam necessários ao pleno atendimento das funcionalidades exigidas neste Contrato;

2.6. A **CONTRATADA** deverá ministrar Treinamento Operacional, Treinamento On-Site e Treinamento Oficial conforme descrito no **ANEXO 1-A** deste Contrato.

2.7. A **CONTRATADA** deverá prestar a garantia e a assistência técnica dos **PRODUTOS** conforme descrito no **ANEXO 1-A** deste Contrato.

2.7.1. Todos os **PRODUTOS** fornecidos deverão possuir garantia de funcionamento durante o período de **48 (quarenta e oito) meses a partir da data do aceite da Fase III.**

2.8. Manter todas as condições de habilitação e qualificação exigidas na licitação, durante todo o período deste Contrato.

2.9. Executar os serviços em estrita observância das especificações e dos detalhamentos constantes dos **ANEXOS 1-A e 1-B** deste Contrato.

2.10. Emitir Nota(s) Fiscal(is) dos serviços efetivamente prestados, apresentando-a(s) à **CONTRATANTE**, conforme descrito no **subitem 5.1.** deste Contrato, discriminando detalhadamente no corpo da(s) Nota(s) Fiscal(is) todos os produtos a que se refere o serviço, o período/fase a que se refere o serviço, o número e o objeto do respectivo Contrato, de acordo com estabelecido no **subitem 1.1.** deste Termo.

2.10.1. Caso a **CONTRATADA** possua mais de um Contrato com a **CONTRATANTE**, deverá emitir Notas Fiscais/Faturas distintas.

2.11. Aceitar, nas mesmas condições contratuais, acréscimos ou supressões que se fizerem necessárias, em até **25% (vinte e cinco por cento)** do valor inicial atualizado deste Contrato previsto no **subitem 4.1.** da **Cláusula Quarta**, facultada a supressão além desse limite, mediante acordo entre as partes.

2.12. Reparar ou corrigir, às suas expensas, no todo ou em parte, os serviços em que se verificarem vícios, defeitos ou incorreções resultantes da execução.

DEPARTAMENTO JURÍDICO Conforme NJ/ DEJUR/ DJTEC

ROS - Avenue 01 CPMI - CORREIOS Fls: 1005

Doc: 3685

2.13. Responder, diretamente, por quaisquer perdas, danos ou prejuízos que vier a causar à **CONTRATANTE** ou a terceiros, decorrentes de sua ação ou omissão, dolosa ou culposa, na execução deste Contrato, independentemente de outras cominações contratuais ou legais a que estiver sujeita.

2.14. Responsabilizar-se por todos e quaisquer ônus e encargos decorrentes da Legislação Fiscal (Federal, Estadual e Municipal) e da Legislação Social, Previdenciária, Trabalhista e Comercial, sendo certo que os empregados da **CONTRATADA** não terão vínculo empregatício com a **CONTRATANTE**.

2.15. A inadimplência da **CONTRATADA**, com referência aos encargos trabalhistas, sociais, previdenciários, fiscais e comerciais, não transfere à **CONTRATANTE** a responsabilidade por seu pagamento, nem poderá onerar o objeto deste Contrato.

2.16. Substituir, sem qualquer ônus para a **CONTRATANTE**, sempre que exigido, e, independente de justificativa por parte desta, qualquer prestador de serviço, cuja atuação, permanência ou comportamento sejam julgados prejudiciais, inconvenientes ou insatisfatórios.

2.17. Apresentar, antes do início das atividades, relação do pessoal a ser alocado nos respectivos serviços, com dados pessoais de identificação e mantê-la rigorosamente atualizada, se for o caso.

2.18. Apresentar, juntamente com a relação de pessoal referente ao item anterior, **Termo de Confidencialidade,** da **CONTRATADA** para com a **CONTRATANTE,** de todas as informações existentes nos ambientes dos Centros Corporativos de Dados da **CONTRATANTE**.

2.19. Disponibilizar para a **CONTRATANTE**, os **PRODUTOS** no prazo de **60 (sessenta)** dias após o término da vigência deste Contrato, a fim de que a **CONTRATANTE** efetue a migração de todos os dados e/ou aplicações armazenados nos **PRODUTOS** contratados.

2.20. Recolher os valores referentes aos **subitens 3.9. e 3.9.1.** da **CLÁUSULA TERCEIRA** deste Termo.

CLÁUSULA TERCEIRA - DAS OBRIGAÇÕES DA CONTRATANTE

3.1. Emitir o **Termo de Aceitação do Cronograma de Trabalho – FASE I**, apresentado pela **CONTRATADA**, no prazo máximo de **10 (dez) dias** de seu recebimento, conforme descrito no **subitem 1.2.** do **ANEXO 1-A** deste Contrato.

3.2. Colocar à disposição da **CONTRATADA** o local onde serão entregues os **PRODUTOS**.

3.3. Emitir o **Termo de Aceitação na Fase III**, em um prazo de até **10 (dez) dias úteis**, conforme descrito no **subitem 1.4.** do **ANEXO 1-A** deste Contrato.

3.4. Efetuar os pagamentos devidos à **CONTRATADA** no prazo estabelecido no **subitem 5.1.** deste Contrato.

3.5. Colocar os **PRODUTOS** à disposição da **CONTRATADA**, para execução da manutenção preventiva e corretiva, sempre que necessário.

DEPARTAMENTO JURÍDICO
Conforme
NJ/DEJUR/DJTEC

RQS nº 03/2003 - CN - CPMI - CORREIOS
1006
Fls:

3685
Doc:

3.6. Fiscalizar a execução deste Contrato e subsidiar a **CONTRATADA** com informações necessárias ao fiel e integral cumprimento contratual.

3.7. Permitir a remoção dos **PRODUTOS** locados pela **CONTRATADA** em um prazo de **60 (sessenta)** dias após o término da vigência deste Contrato.

3.8. Comunicar à **CONTRATADA** toda e qualquer ocorrência que interfira na execução dos serviços.

3.9. Disponibilizar, a pedido da **CONTRATADA**, linha(s) telefônica(s), com recurso de bloqueio por senha, para seu uso exclusivo, permitindo originar e receber chamadas DDD e DDI durante o período de vigência do Contrato.

3.9.1. Os valores referentes ao uso dos ramais disponibilizados para a **CONTRATADA**, deverão ser recolhidos nas agências dos Correios, por meio de CR - Comprovante de Recebimento, até o **15º (décimo quinto) dia útil** do mês subsequente a apresentação da fatura; o não recolhimento implicará na glosa desses valores, na próxima fatura referente à locação mensal.

CLÁUSULA QUARTA – DO VALOR E DOS PREÇOS

4.1. O valor global do presente Contrato é de **R$ 106.036.869,19 (cento e seis milhões, trinta e seis mil, oitocentos e sessenta e nove reais e dezenove centavos)**, conforme disposto na forma abaixo:

4.1.1. R$ 104.986.999,20 (cento e quatro milhões, novecentos e oitenta e seis mil, novecentos e noventa e nove reais e vinte centavos) referente ao valor global da locação dos produtos;

4.1.2. R$ 1.049.869,99 (hum milhão, quarenta e nove mil, oitocentos e sessenta e nove reais e noventa e nove centavos) equivalente a 1% (um por cento) do VALOR TOTAL DA LOCAÇÃO referente a Apresentação do Cronograma de Trabalho;

4.1.3. Conforme pauta constante no **ANEXO 1-B**, o valor global da locação dos produtos está assim distribuído:

a) Diretoria Regional de São Paulo Metropolitana: R$ 35.314.128,35 (trinta e cinco milhões, trezentos e catorze mil, cento e vinte e oito reais e trinta e cinco centavos), referente aos **PRODUTOS** locados para o Centro Corporativo de Dados de São Paulo Metropolitana, sendo:

a1) Locação mensal dos produtos nos 48 (quarenta e oito) meses: R$ 728.426,74 (setecentos e vinte e oito mil, quatrocentos e vinte e seis reais e setenta e quatro centavos);

a2) Apresentação do Cronograma de Trabalho: R$ 349.644,83 (trezentos e quarenta e nove mil, seiscentos e quarenta e quatro reais e oitenta e três centavos);

b) Administração Central: R$ 70.722.740,84 (setenta milhões, setecentos e vinte e dois mil, setecentos e quarenta reais e oitenta e quatro centavos), referente aos **PRODUTOS** locados para o Centro Corporativo de Brasília/AC, sendo:

b1) Locação mensal dos produtos nos 48 (quarenta e oito meses): R$ 1.458.802,11 (hum milhão, quatrocentos e cinqüenta e oito mil, oitocentos e dois reais e onze centavos);

DEPARTAMENTO JURÍDICO
Conforme
DJ/DEJUR/DJTEC

RQS nº 03/2003 - CN - CORREIOS
1007
Fls:
3685
Doc:

b2) Apresentação do Cronograma de Trabalho: R$ 700.225,16 (setecentos mil, duzentos e vinte e cinco reais e dezesseis centavos).

4.1.2. Os preços mensais unitários de locação de cada **PRODUTO**, incluindo a instalação, a configuração, o treinamento, a assistência técnica e a garantia, com base na data da abertura da proposta, 24/07/2003, estão discriminados na proposta da **CONTRATADA**.

4.2. As despesas com passagens, diárias, alimentação, hospedagem e outras despesas com seus empregados, serão de responsabilidade da **CONTRATADA**.

4.3. No preço estão contidos todos os custos e despesas diretas e indiretas, tributos incidentes, assistência técnica aos **PRODUTOS** e garantia, encargos sociais, previdenciários, trabalhistas e comerciais, taxa de administração e lucro, materiais e mão-de-obra a serem empregados, seguros, frete, embalagens, despesas com transporte, hospedagem, diárias, alimentação e quaisquer outros, obrigatórios ou necessários à composição do preço do objeto deste Contrato.

4.4. O preço é fixo e irreajustável durante os **12 (doze) primeiros meses** da locação, salvo se houver determinação do Poder Executivo em contrário e de acordo com as regras a serem definidas à época.

CLÁUSULA QUINTA - DO PAGAMENTO

5.1. Os pagamentos serão efetuados conforme demonstrado abaixo, mediante apresentação de Nota(s) Fiscal(is)/Fatura(s) devidamente atestada(s) pela **CONTRATANTE**:

5.1.1. Apresentação do Cronograma de Trabalho, que será pago em única parcela no **15º (décimo quinto) dia** após a data de emissão do **Termo de Aceitação da Fase I**.

5.1.2. mensalmente referente aos **48 (quarenta e oito)** meses de alugueres, no **15º (décimo quinto) dia** do mês subseqüente ao da prestação dos serviços, após a emissão do **Termo de Aceitação da Fase III**, conforme descrito no **ANEXO 1-A** deste Contrato

5.2. Os faturamentos emitidos pela **CONTRATADA,** referentes ao CCD Brasília e CCD São Paulo, deverão ser apresentados a partir do **1º (primeiro) dia** útil do mês subseqüente ao início da locação, assim como o faturamento do **subitem 5.1.1.**, após o recebimento do termo de aceitação, nos endereços descritos abaixo:

a) AC – Administração Central
DPROD – DEPARTAMENTO DE OPERACAO E PRODUÇÃO – ECT
Endereço: SBN Quadra 01 Conjunto 03 Bloco A, Ed. Sede da ECT – 2º Subsolo
CEP: 70002-900 – Brasília/DF

a1) O gestor técnico/operacional atestará a prestação dos serviços e encaminhará em tempo hábil, ao Departamento de Suporte a Administração Central, para providências de pagamento, providenciando, ainda, o envio de cópia de documento fiscal, devidamente atestado, à Divisão de Gestão de Contratos do DECAM.

b) DR/SPM – Diretoria Regional de São Paulo Metropolitana
GESIT – GERÊNCIA DE SISTEMAS DE TELEMÁTICA
Endereço: Rua Mergenthaler, 592 – Bloco 2 – 7º andar
CEP: 05311-900 – São Paulo/SP

b1) O gestor técnico/operacional atestará a prestação dos serviços e encaminhará em tempo hábil, à Gerência de Administração-GERAD/DR/SPM, para providências de pagamento, providenciando, ainda, o envio de cópia de documento fiscal, devidamente atestado, à Divisão de Gestão de Contratos do DECAM.

5.3. Havendo disponibilidade e interesse da **CONTRATANTE**, bem como solicitação da **CONTRATADA,** o pagamento eventualmente poderá ser antecipado, mediante desconto, nos termos do Art. 40, Inciso XIV, letra "d" da Lei 8.666/93 e nas regras estabelecidas no site da ECT, acessando http://www.correios.com.br/institucional/licit_compras_contratos/SPFVP/default.cfm.

5.4. Para fins de pagamento, deverá(ao), ainda, ser apresentado(s), juntamente com a Nota Fiscal/Fatura, a Certidão Negativa de Débito do INSS, devidamente atualizada;

5.4.1. A não-apresentação da Certidão Negativa de Débito do INSS (CND), ou sua irregularidade, não acarretará retenção do pagamento. Entretanto, a **CONTRATADA** será comunicada quanto à apresentação de tal documento em até **30 (trinta) dias**, sob pena de rescisão contratual e demais penalidades cabíveis.

5.4.2. Decorrido o prazo acima, persistindo a irregularidade, o Contrato poderá ser rescindido, sem prejuízo das demais penalidades cabíveis.

5.4.3. Concomitante à comunicação à **CONTRATADA,** a **CONTRATANTE** oficiará a ocorrência ao INSS.

5.5. Caso o serviço não seja prestado fielmente e/ou o documento fiscal apresente alguma incorreção, será considerado como não aceito e o prazo de pagamento será contado a partir da data de regularização, observado o prazo disposto no **subitem 5.1.** deste Contrato.

5.6. O(s) pagamento(s) será(ão) efetuado(s) por meio de depósito bancário, conforme dados a seguir:

BANCO: Itaú S/A
AGÊNCIA: 0912
CONTA CORRENTE: 08067-8

5.7. Quaisquer alterações nos dados bancários deverão ser comunicadas à **CONTRATANTE**, por meio de Carta, ficando sob inteira responsabilidade da **CONTRATADA** os prejuízos decorrentes de pagamentos incorretos devido à falta de informação.

5.8. Correrão por conta da **CONTRATADA** o ônus do prazo de compensação e todas as despesas bancárias decorrentes da transferência de crédito.

5.9. Ocorrendo atraso de pagamento, por culpa da **CONTRATANTE,** será procedida a atualização monetária decorrente desse atraso, com base na variação *pro rata tempore* do IGPM (FGV), verificada entre a data prevista para pagamento e a data em que o mesmo foi efetivado.

5.10. A **CONTRATANTE** não acatará a cobrança por meio de duplicatas ou qualquer outro título, em bancos ou outras instituições do gênero.

5.11. Os pagamentos efetuados pela **CONTRATANTE** não isentam a **CONTRATADA** de suas obrigações e responsabilidades assumidas.

DEPARTAMENTO JURÍDICO E.C.T. Conforme NJ/DEJUR/DJTEC

CPMI - CORREIOS Fls: 1009 3685 Doc:

5.12. Não havendo expediente na **CONTRATANTE**, a data de vencimento da obrigação será prorrogada para o primeiro dia útil imediato.

CLÁUSULA SEXTA – DO REAJUSTE

6.1. As alterações do valor da parcela mensal de locação acordado neste Contrato deverão atender às disposições da Resolução n º 10 de 08/10/96, do Conselho de Coordenação e Controle das Empresas Estatais (CCE) que poderão ocorrer na seguinte hipótese:

6.1.1. Decorridos **12 (doze) meses** de locação, após a data de emissão do **TERMO DE ACEITAÇÃO** da **Fase III**, mediante reajuste dos preços, tendo por parâmetros básicos a qualidade da prestação dos serviços e os preços vigentes no mercado, devendo a **CONTRATADA** apresentar solicitação formal, indicando o valor a ser reajustado.

6.2. Na negociação de preços para reajuste deverá ser observada como limitador a manutenção da relação existente entre preços pactuados e preços de mercado, quando da apresentação da proposta de origem.

6.3. Caso o reajuste de preços não seja requerido no prazo previsto no **subitem 6.1.1.**, poderá ocorrer a qualquer momento, desde que decorridos os **12 (doze) primeiros meses** de locação ou do último reajuste.

CLÁUSULA SÉTIMA – DAS ALTERAÇÕES CONTRATUAIS

7.1. Este Contrato poderá ser alterado, com as devidas justificativas, nos seguintes casos:

7.1.1. ***Unilateralmente,*** pela **CONTRATANTE**, quando:

a) houver modificação do projeto ou das especificações, para melhor adequação técnica aos seus objetivos;

b) necessária à modificação do valor contratual em decorrência de acréscimo ou diminuição quantitativa de seu objeto, nos limites previstos neste Contrato.

7.1.2. ***Por acordo entre as partes***, quando:

a) necessária à modificação do regime de execução do serviço, bem como do modo ou cronograma do serviço, em face de verificação técnica da inaplicabilidade dos termos contratuais originários;

b) necessária à modificação da forma de pagamento, por imposição de circunstâncias supervenientes, mantido o valor inicial atualizado, vedada a antecipação do pagamento, com relação ao cronograma financeiro fixado, sem a correspondente contraprestação de execução dos serviços;

c) para restabelecer a relação que as partes pactuaram inicialmente entre os encargos da **CONTRATADA** e a retribuição da **CONTRATANTE** para a justa remuneração dos serviços, objetivando a manutenção do equilíbrio econômico-financeiro inicial deste Contrato, na hipótese de sobrevirem fatos imprevisíveis ou previsíveis, porém de conseqüências incalculáveis, retardadores ou impeditivos da execução do ajustado, ou ainda em caso de força maior, caso fortuito ou fato do príncipe, configurando álea econômica extraordinária e extracontratual.

ROS nº 02/2005 - CN - CPMI - CORREIOS
1010
Fls:
DEPARTAMENTO JURÍDICO
Conforme
NJ/DEJUR/DJTEC 3685
Doc:

d) conveniente à substituição da garantia de execução contratual.

7.2. As alterações serão procedidas mediante os seguintes instrumentos:

7.2.1. APOSTILAMENTO: para as alterações que envolverem as seguintes situações:

a) a variação do valor contratual para fazer face ao reajuste de preços, previsto no próprio Contrato;

b) as atualizações, compensações ou penalizações financeiras decorrentes das condições de pagamento aqui previstas;

c) o empenho de dotações orçamentárias suplementares, até o limite do seu valor corrigido;

d) ajustes nas especificações, no cronograma de entrega ou na execução dos serviços, desde que não impactem nos encargos contratados e não afetem a isonomia do processo licitatório, situações estas, previamente, reconhecidas por autoridade competente da **CONTRATANTE**.

7.2.2. TERMO ADITIVO: alterações não abrangidas pelo apostilamento, que ensejarem modificações deste Contrato ou do seu valor, para que prorrogações de vigências contratuais previstas neste Contrato.

7.3. Os Termos Aditivos ou Apostilas farão parte deste Contrato, como se nele estivessem transcritos.

CLÁUSULA OITAVA - DAS PENALIDADES

8.1. Pela inexecução total ou parcial deste Contrato, a **CONTRATANTE** poderá aplicar à **CONTRATADA** as seguintes sanções, sem prejuízo da reparação dos danos causados à **CONTRATANTE**:

8.1.1. Advertência: será aplicada quando ocorrer o descumprimento das obrigações assumidas, desde que sua gravidade, devidamente analisada e justificada pela **CONTRATANTE**, não recomende a aplicação de outra penalidade.

8.1.2. Multa: será aplicada nos seguintes casos:

8.1.2.1. O atraso injustificado na execução deste Contrato sujeitará a **CONTRATADA** à **multa de mora**, na forma a seguir:

a) pelo atraso na entrega do Cronograma de Trabalho: **1% (um por cento)**, por dia corrido, do valor previsto no **subitem 5.1.1.** deste Termo;

b) pelo atraso na conclusão da Fase III, definido no **subitem 2.3. da clausula Segunda** deste Termo: **1% (um por cento)**, por dia corrido, do **VALOR MENSAL DA LOCAÇÃO**, referente ao primeiro mês;

c) pelo atraso na reparação/substituição dos equipamentos defeituosos ou que apresentarem mau funcionamento durante o **PFE - Período de Funcionamento Experimental**, comprometendo o perfeito funcionamento e a aceitação do ambiente: **0,2% (zero vírgula dois por cento)**, por dia corrido, do **VALOR TOTAL DA LOCAÇÃO** dos equipamentos contratados, até o limite de **30 (trinta) dias**;

REG. Nº 3685 CPMI - CORREIOS

DEPARTAMENTO JURÍDICO

1011 Fls.

Conforme 3685

AJ/DEJUR/DJTEC ____/____

Doc:

d) a partir do **31º (trigésimo primeiro) dia** de atraso na reparação/substituição dos equipamentos defeituosos ou que apresentarem mau funcionamento durante o **PFE - Período de Funcionamento Experimental**, comprometendo o perfeito funcionamento e a aceitação do ambiente: **0,4 (zero vírgula quatro por cento)**, por dia corrido, do **VALOR TOTAL DA LOCAÇÃO** dos produtos contratados;

e) pelo atraso na realização do treinamento a ser ministrado pela **CONTRATADA**: **0,5% (meio por cento)**, por dia corrido, do **VALOR MENSAL DA LOCAÇÃO**;

f) pelo atraso no início do atendimento para reparação do defeito nos produtos: SERVIDORES RISC TIPO 01, SERVIDORES INTEL TIPO 01, SWITCHES TIPO 01, SWITCHES TIPO 03 E UNIDADES DE BACKUP ROBOTIZADO, **2,5% (dois virgula cinco por cento)**, por hora de atraso, do **VALOR MENSAL DA LOCAÇÃO** do(s) produto(s) afetado(s), observado os prazos estabelecidos no **subitem 1.8.1.** e **1.8.2. do ANEXO 1-A**;

g) pelo atraso no início do atendimento para reparação do defeito nos demais produtos: **1% (um por cento)**, por hora de atraso, do **VALOR MENSAL DA LOCAÇÃO** do(s) produto(s) afetado(s), observado os prazos estabelecidos no **subitem 1.8.1.** e **1.8.2. do ANEXO 1-A**;

h) pelo atraso na solução total do problema, de forma a recolocar em plenas condições de operação os produtos: SERVIDORES RISC TIPO 01, SERVIDORES INTEL TIPO 01, SWITCHES TIPO 01, SWITCHES TIPO 03 E UNIDADES DE BACKUP ROBOTIZADO: **5% (cinco por cento)**, por hora de atraso, do **VALOR MENSAL DA LOCAÇÃO** do(s) produto(s) afetado(s), observado os prazos estabelecidos no **subitem 1.8.1.** e **1.8.2. do ANEXO 1-A**;

i) pelo atraso na solução total do problema, de forma a recolocar em plenas condições de operação os demais produtos: **2,5% (dois virgula cinco por cento)**, por hora de atraso, do **VALOR MENSAL DA LOCAÇÃO** do(s) produto(s) afetados(s), observado os prazos estabelecidos no **subitem 1.8.1.** e **1.8.2. do ANEXO 1-A**;

j) pelo atraso na substituição dos equipamentos ou do componente defeituoso, por outro de propriedade da **CONTRATADA**, nos termos do **subitem 1.8.1. do ANEXO 1-A** deste Contrato que trata da garantia de funcionamento: **1% (um por cento)**, por hora de atraso, do **VALOR MENSAL DA LOCAÇÃO**;

k) não-cumprimento de quaisquer condições de garantia do serviço, estabelecidas no **ANEXO 1-A**: **1% (um por cento)**, por dia corrido, do **VALOR MENSAL DA LOCAÇÃO**.

8.1.2.2. Pela inexecução total ou parcial serão aplicadas multas na forma a seguir, garantida a prévia defesa:

a) pela não-observação da disponibilidade mínima do(s) produtos(s), nos termos do **subitem 1.5. do ANEXO 1-A** deste Contrato: **2% (dois por cento)** do **VALOR MENSAL DA LOCAÇÃO** de cada produto em questão;

b) ocorrência de quaisquer outros tipos de descumprimento contratual não abrangidos pelas demais alíneas: **1% (um por cento)** do **VALOR MENSAL DA LOCAÇÃO,** atualizado, para cada evento, por dia corrido;

c) quando a **CONTRATADA** incorrer em alguma das hipóteses das alíneas **"a"**, **"a1"**, **"a2"** ou **"d"** a **"k"** do **subitem 9.1.1.** deste Contrato: **20% (vinte por cento)** do **VALOR TOTAL DA LOCAÇÃO**, atualizado;

DEPARTAMENTO JURÍDICO DECT Conforme MJ/DEJUN/DJTEC

Fls: 3685 Doc:

d) não-apresentação/atualização da garantia de execução contratual, estabelecida neste Contrato: **1% (um por cento)** do **VALOR TOTAL DA GARANTIA PRESTADA**, por dia de atraso, conforme **subitem 14.1.** deste Contrato.

8.1.2.3. As multas previstas nos **subitens 8.1.2.1. e 8.1.2.2.** são independentes entre si, podendo ser aplicadas isoladas ou cumulativamente, ficando, porém, o total delas limitado a **20% (vinte por cento)** do **VALOR TOTAL DA LOCAÇÃO**, atualizado.

8.1.2.4. Em caso de descumprimento deste Contrato, além das multas de mora, a **CONTRATADA** responderá por quaisquer danos e prejuízos sofridos pela **CONTRATANTE.**

8.1.2.5. Não serão aplicadas multas decorrentes de casos fortuitos, ou força maior, ou razões de interesse público, devidamente comprovados.

8.1.2.6. O valor da multa e os prejuízos causados pela **CONTRATADA** serão executados pela **CONTRATANTE**, nos termos das alíneas **"a"**, **"b"** e **"c"** do **subitem 9.6.** deste Contrato.

8.1.3. Suspensão temporária de participação em licitação e impedimento de contratar com a CONTRATANTE: pelo período de 6 (seis) meses a 2 (dois) anos, ou, no caso de Pregão, não superior a **5 (cinco) anos**, poderá ser aplicada nos seguintes casos:

a) não-manutenção de situação regular em relação à Documentação de Habilitação;

b) se a **CONTRATADA** der causa à rescisão unilateral deste Contrato, por descumprimento de suas obrigações;

c) apresentação de documentos falsos ou falsificados;

d) cometimento reiterado de falhas ou fraudes na execução deste Contrato.

8.1.3.1. A suspensão temporária de participação em licitação e impedimento de contratar com a **CONTRATANTE,** também, poderá ser aplicada nos casos previstos nas alíneas do **subitem 8.1.4.**

8.1.4. Declaração de inidoneidade para licitar ou contratar com a Administração Pública enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação perante a própria autoridade que aplicou a penalidade, que será concedida sempre que a **CONTRATADA** ressarcir a Administração pelos prejuízos resultantes e após decorrido o prazo previsto no § 3º, do Art. 87, da Lei nº 8.666/93, que será aplicada, também, nos seguintes casos:

a) tenha sofrido condenação definitiva por praticar, por meios dolosos, fraude fiscal no recolhimento de quaisquer tributos;

b) tenha praticado atos ilícitos, visando a frustrar os objetivos da contratação;

c) demonstre não possuir idoneidade para contratar com a Administração Pública;

8.2. As penalidades serão aplicadas com observância aos princípios da ampla defesa e do contraditório.

8.3. No caso do **subitem 8.1.2.1**, a multa será aplicada de imediato, sendo deduzida do valor da Nota Fiscal/Fatura.

ROS nº 03/2005 - CN - CPMI - CORREIOS
Fls: 1013
3685
Doc:

DEPARTAMENTO JURÍDICO
Conforme
MJ/DEJUR/DJTEC ____/____

8.4. As sanções previstas nos **subitens 8.1.1., 8.1.3. e 8.1.4.** poderão ser aplicadas juntamente com a do **subitem 8.1.2.**, facultada a defesa prévia da **CONTRATADA**, no prazo de **5 (cinco) dias úteis**, cujas razões, em sendo procedentes, poderão isentá-la das penalidades; caso contrário, aplicar-se-á a sanção cabível.

8.5. Da aplicação das penalidades previstas nesta Cláusula caberá recurso.

8.5.1. O recurso será dirigido à autoridade superior, por intermédio da que praticou o ato recorrido, a qual poderá reconsiderar sua decisão, no prazo de **5 (cinco) dias úteis**, ou, neste mesmo prazo, fazê-lo subir, devidamente informado, devendo, neste caso, a decisão ser proferida em **5 (cinco) dias úteis** contados do recebimento do recurso, pela autoridade superior, sob pena de responsabilidade.

CLÁUSULA NONA - DA RESCISÃO

9.1. O presente Contrato poderá ser rescindido, sem prejuízo das penalidades previstas na Cláusula Oitava:

9.1.1. Por ato unilateral da **CONTRATANTE**, quando ocorrer:

a) o não-cumprimento ou cumprimento irregular de Cláusulas contratuais, especificações, projetos ou prazos;

a1) não-manutenção das condições de habilitação exigidas na licitação;

a2) descumprimento do disposto no Inciso V do Art. 27 da Lei 8.666/93, sem prejuízo das sanções penais cabíveis;

b) a lentidão do seu cumprimento, levando a **CONTRATANTE** a comprovar a impossibilidade da conclusão do serviço, nos prazos estipulados;

c) atraso injustificado na execução dos serviços, impossibilitando a **ACEITAÇÃO FINAL** dos equipamentos por parte da **CONTRATANTE**;

d) não reparação/substituição dos equipamentos defeituosos ou que apresentarem mau funcionamento durante o PFE - Período de Funcionamento Experimental, comprometendo o perfeito funcionamento e a aceitação do ambiente;

e) paralisação do serviço, sem justa causa e prévia comunicação à **CONTRATANTE**;

f) subcontratação total ou parcial do objeto deste Contrato, ou a associação da **CONTRATADA** com outrem, cessão ou transferência, total ou parcial, bem como a fusão, cisão ou incorporação, sem expressa anuência da **CONTRATANTE**;

g) desatendimento das determinações regulares da autoridade designada para acompanhar e fiscalizar a sua execução, assim como, a de seus superiores;

h) cometimento reiterado de falhas na execução deste Contrato;

i) decretação de falência da **CONTRATADA**;

j) dissolução da sociedade da **CONTRATADA**;

k) alteração social ou a modificação da finalidade ou da estrutura da **CONTRATADA**, que prejudique a execução deste Contrato;

l) razões de interesse público, de alta relevância e amplo conhecimento, justificadas e determinadas pela máxima autoridade da esfera administrativa a que está subordinada a **CONTRATANTE** e exaradas no processo administrativo a que se refere este Contrato;

m) caso fortuito ou força maior, regularmente comprovados, impeditivos à execução deste Contrato.

9.1.2. Amigavelmente, por acordo entre as partes, desde que haja conveniência para a **CONTRATANTE**, reduzida a termo no Processo Administrativo.

9.1.3. Judicialmente, nos termos da legislação.

9.2. É prevista a rescisão, ainda, nos seguintes casos:

a) supressão, por parte da **CONTRATANTE**, acarretando modificação além do limite de **25% (vinte e cinco por cento)** do valor inicial atualizado deste Contrato, estabelecido à época da celebração deste Instrumento, devidamente corrigido até a data da supressão, ressalvados os casos de concordância da **CONTRATADA**;

b) suspensão de sua execução, por ordem escrita da **CONTRATANTE**, por prazo superior a **120 (cento e vinte) dias**, salvo em caso de calamidade pública, grave perturbação da ordem interna ou guerra, ou ainda, por repetidas suspensões que totalizem o mesmo prazo, independentemente do pagamento obrigatório de indenização pelas sucessivas e contratualmente imprevistas desmobilizações e mobilizações e outras previstas, assegurado à **CONTRATADA**, nesses casos, o direito de optar pela suspensão do cumprimento das obrigações assumidas até que seja normalizada a situação;

c) ocorrendo atraso superior a **90 (noventa) dias** dos pagamentos devidos pela **CONTRATANTE**, salvo em caso de calamidade pública, grave perturbação da ordem interna ou guerra, assegurado à **CONTRATADA** o direito de optar pela suspensão do cumprimento de suas obrigações até que seja normalizada a situação.

9.3. Os casos de rescisão contratual serão formalmente motivados nos autos do Processo Administrativo, assegurado o contraditório e a ampla defesa.

9.4. A rescisão unilateral ou amigável deverá ser precedida de autorização escrita e fundamentada da autoridade competente.

9.5. Quando a rescisão ocorrer com base nas alíneas "l" e "m" do **subitem 9.1.1.,** desta Cláusula e alíneas "a", "b" e "c" do subitem 9.2., sem que haja culpa da **CONTRATADA**, será esta ressarcida dos prejuízos regularmente comprovados que houver sofrido.

9.6. A rescisão de que trata o **subitem 9.1.1.,** exceto quando se tratar de casos fortuitos, ou força maior ou razões de interesse público, acarretará as seguintes conseqüências, sem prejuízo das sanções previstas em lei ou neste instrumento:

a) retenção dos créditos decorrentes deste Contrato, até o limite dos prejuízos causados à **CONTRATANTE**;

DEPARTAMENTO JURÍDICO
Conforme
MJ/DEJUR/DJTEC

b) retenção dos créditos existentes em outros Contratos, porventura vigentes entre a **CONTRATANTE** e a **CONTRATADA,** até o limite dos prejuízos causados;

c) retenção/execução da garantia contratual, para ressarcimento da **CONTRATANTE** dos valores das multas e indenizações a ela devidos.

9.7 Caso a retenção não possa ser efetuada, no todo ou em parte, na forma prevista nas alíneas do **subitem 9.6.**, a **CONTRATADA** será notificada para, no prazo de **5 (cinco) dias úteis,** a contar do recebimento da notificação, recolher o respectivo valor em Agência indicada pela **CONTRATANTE**, sob pena de imediata aplicação das medidas judiciais cabíveis.

CLÁUSULA DÉCIMA - DOS RECURSOS ORÇAMENTÁRIOS

10.1. As despesas decorrentes da prestação de serviços, objeto deste Contrato, correrão por conta da seguinte classificação orçamentária:

Conta: 800.07.03.0000 – Atividade: 00.8.00.

CLÁUSULA DÉCIMA-PRIMEIRA - DA VIGÊNCIA

11.1. O período de vigência do presente Contrato se inicia na data da sua assinatura, prolongando-se até **48 (quarenta e oito) meses**, a contar da data da emissão do Termo de Aceitação da Fase III.

CLÁUSULA DÉCIMA-SEGUNDA - DA LICITAÇÃO E SUBORDINAÇÃO LEGAL

12.1. Este Contrato é oriundo do Pregão n.º 050/2003-CPL/AC, homologado na REDIR-030/2003, por meio do Relatório/DITEC-028/2003 de 30/07/2003.

12.2. As partes contratantes submetem-se às condições ora acordadas e aos ditames da Lei nº 10.520/2002, do Decreto nº 3.555/00 e, supletivamente, Lei nº 8.666/93.

12.3. Constituirão partes integrantes deste Contrato: seus **ANEXOS (ANEXO 1-A e 1-B)**, o Edital, seus Anexos, e a Proposta Econômica da **CONTRATADA**.

12.4. A **CONTRATANTE** providenciará a publicação do extrato do presente Contrato na imprensa oficial, nos termos da legislação vigente.

RQS nº 03/2006 - CN
CPMI - CORREIOS
1016
Fls:
3685
Doc:

CLÁUSULA DÉCIMA-TERCEIRA - DA GESTÃO DO CONTRATO

13.1. A gestão deste Contrato será feita:

13.1.1 Por parte da **CONTRATANTE:**

ÁREA GESTORA OPERACIONAL: DEPARTAMENTO DE OPERAÇÃO E PRODUÇÃO/DPROD
TELEFONE: (61) 426-2214/2198
FAX: (61) 426-2206

ÁREA GESTORA ADMINISTRATIVA: DIVISÃO DE GESTÃO DE CONTRATOS/DGEC/DECAM
TELEFONE: (61) 426-2774/2795
FAX: (61) 426-2807

DEPARTAMENTO JURÍDICO DEJUR T
Conforme
DJ/DEJUR/DJTEC ____/____

13.1.2. Por parte da **CONTRATADA:**

NOME DO GESTOR: JOSÉ EDUARDO PIRES DO RIO RIBEIRO
ENDEREÇO: SCN Quadra 02 Bloco A – 5º andar – Sala 51 – Ed. Corporate
TELEFONE: (61) 329-6055/9974-6565
FAX: (61) 329-6199
E-MAIL: jose-eduardo.ribeiro@hp.com

13.2. o **ANEXO 1** deste Contrato será igual ao **ANEXO 1 (ANEXO 1, 1-A e 1-B)** do Edital, ressalvadas as condições já constantes no corpo deste Contrato.

CLÁUSULA DÉCIMA-QUARTA - DA GARANTIA DE EXECUÇÃO CONTRATUAL

14.1. A **CONTRATADA** comprovará no prazo de **05 (cinco) dias úteis** da data de assinatura deste Contrato, a efetivação da garantia de execução contratual, que deverá corresponder à vigência do presente Instrumento, em percentual equivalente a **3% (três por cento)** do valor global, correspondente a **R$ 3.181.106,07 (três milhões, cento e oitenta e um mil, cento e seis reais e sete centavos)** , podendo optar por uma das seguintes modalidades:

a) caução em dinheiro ou títulos da dívida pública;
b) seguro-garantia;
c) fiança bancária.

14.2. Em caso de garantia em dinheiro, a **CONTRATADA** deverá depositar o valor em nome da **CONTRATANTE**, conforme dados abaixo:

BANCO: Banco do Brasil S/A (001)
AGÊNCIA: 3307-3
CONTA CORRENTE: 195.159-9

14.3. No caso de apresentação de fiança bancária, a Carta de Fiança deverá registrar expressa renúncia do fiador aos benefícios dos artigos 827 e 835 do Novo Código Civil Brasileiro.

14.4. Se a opção da garantia recair em seguro garantia ou fiança bancária, deverá conter expressamente cláusulas de atualização financeira, de imprescritibilidade, de inalienabilidade e de irrevogabilidade.

14.5. A garantia apresentada na modalidade de Seguro somente será considerada válida após a entrega das apólices à **CONTRATANTE.**

14.6. Se o valor da garantia for utilizado em pagamento de quaisquer obrigações, inclusive indenização a terceiros, a **CONTRATADA** se obriga a fazer a respectiva reposição, no prazo máximo e improrrogável de **72 (setenta e duas) horas**, a contar da data que for notificada pela **CONTRATANTE**.

14.7. A garantia prestada será liberada ou restituída após a vigência deste Contrato, desde que cessadas todas as obrigações assumidas pela **CONTRATADA**.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1017
Conforme 3685
NJ/DEJUR/DJTEC
Doc:

DEPARTAMENTO JURÍDICO

CLÁUSULA DÉCIMA - QUINTA - DO FORO

15.1. É competente o Foro da Justiça Federal, Seção Judiciária do Distrito Federal, para dirimir quaisquer dúvidas, porventura oriundas do presente Contrato.

E, por estarem justas e contratadas, assinam as partes o presente Contrato, em 02 (duas) vias de igual teor e forma e para um só efeito de direito, na presença de 02 (duas) testemunhas abaixo assinadas.

Brasília/DF, 12 de AGOSTO de 2003.

PELA CONTRATANTE

AIRTON LANGARO DIPP
Presidente da ECT

EDUARDO MEDEIROS DE MORAIS
Diretor de Tecnologia e Infra-Estrutura da ECT

PELA CONTRATADA

JOSÉ EDUARDO PIRES DO RIO RIBEIRO
Representante da HP BRASIL LTDA

IVO ROMANI
Representante da HP BRASIL LTDA

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls: 1018
3685
Doc:

TESTEMUNHAS:

1) Karina Spridião Ribeiro
NOME:
CPF: 801815901-53

2) Gabriele Rosa de Alcântara
NOME:
CPF: 334.038.131-34

DEPARTAMENTO JURÍDICO E C T
Conforme
NJ/DEJUR/DJTEC ... / ...

CORREIOS

CORREIOS/ECT -29-Jun-2004-11:21-011748-1/1

De: DECAM

Protocolo

Ao: PREGOEIRA E PRESIDENTE CPL

CI / ASS/DECAM - 1131/2004

Ref.: CI/CPL/AC-0667/2004

Assunto: Auditoria Interna

Brasília, 24 de Junho de 2004.

Em atenção ao expediente acima referido, estamos encaminhando a V.Sª. os documentos relativos aos processos licitatórios abaixo relacionados, os quais dizem respeito ao DECAM:

- Pregão 043/2003 – Aquisição de Cartuchos para Impressoras;
- Pregão 050/2003 – Locação de Equipamentos de Informática;
- Pregão 091/2003 – Aquisição de Microcomputadores;
- Pregão 107/2003 - Fornecimento de Equipamentos para o SRO;
- Pregão Eletrônico 117/2003 – Aquisição de Etiquetas Auto Adesivas;
- Pregão 122/2003 – Aquisição de Witches para Beckbone;
- Pregão Eletrônico 124/2003 – Aquisição de Impressos de Segurança;
- Pregão Eletrônico 130/2003 – Aquisição de Veículos;
- Pregão Eletrônico 131/2003 – Locação de Copiadoras Digitais
- Concorrência 005/2003 - Manutenção Preventiva Sistema PABX

Atenciosamente,

Mauricio Marinho
Chefe do Departamento de Contratação e Administração de Material

Antônio Francisco da Silva Filho
Subchefe/DECAM
Mát. [illegible]819-9

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls: 1019
3685
Doc:

CORREIOS

URGENTE

Protocolo

De: PREGOEIRA E PRESIDENTE DA CPL/AC

Ao: DECAM e DESAD

CI / CPL/AC - 0667/2004

Ref.:

Assunto: Auditoria Interna

Brasília, 28 de junho de 2004.

No período de 22/03 a 28/05/2004, foi realizada Auditoria Interna nesta CPL, em diversos processos concluídos no ano de 2003. Um dos tópicos mais citados no relatório da Auditoria, foi a falta na pasta dos processos das cópias das Atas de Registro de Preços, Termos de Contratos ou AF, já firmados, bem como dos extratos das publicações no Diário Oficial da União.

De se salientar que tal atribuição do DESAD é sempre relembrada, quando encaminhamos os processos para a contratação, conforme preceitua a CI/PR – 005/2002.

Assim, visando o atendimento das determinações da Auditoria, solicitamos:

1) **De modo imediato: (até 29/06)** remeter-nos cópias dos instrumentos contratuais e publicações relativos aos processos a seguir, a fim de que jutarmos às pastas e liquidarmos os pontos de auditoria:

- Pregão 027/2003 – Contratação de Serviços de Recepcionistas – DESAD
- Pregão 043/2003 – Aquis. Cartuchos P/Impress. Canon 210 e 4000 – DECAM
- Pregão 045/2003 – Contratação de Serviço de Copeira e Ascensoristas – DESAD
- Pregão 050/2003 – Locação de 162 Equip. de Informática – DECAM
- Pregão 091/2003 – Aquisição de Microcomputadores - DECAM
- Pregão 093/2003 – Contratação Segurança Patrimonial - DESAD
- Pregão 107/2003 – Fornecimento de Equipamentos para o SRO – DECAM
- Prg Eletr. 117/2003 – Aqui. de Etiq. Auto Adesivas C/ Dados Variáveis – DECAM
- Pregão 122/2003 – Aquisição de Whitches para Beckbone – DECAM
- Prg Eletr 124/2003 – Aquisição de Impressos Segurança - DECAM
- Prg Eletr 130/2003 – Aquisição de Veículos - DECAM
- Prg Eletr 131/2003 – Locação de 21 Copiadoras Digitais - DECAM
- Conc. 005/2003 - Manutenção Preventiva Sistema PABX - DECAM
- Convite 004/2003 – Aquisição de Café e Açúcar — DESAD
- Convite 025/2003 – Aquis. de 250 Certificados de Conclusão de Cursos - DESAD

2) **Perenemente:** que sejam arquivados na pasta dos processos os instrumentos contratuais (após a assinatura) e publicações relativos aos processos licitatórios, conforme preceitua a CI/PR – 005/2002

CORREIOS

Neste contexto , contamos com os habituais préstimos

Atenciosamente,

Marta Maria Coelho
Pregoeira/AC

Tânia Regina Teixeira Munari
Presidente da CPL

PAGINAÇÃO DO PROCESSO

DOCUMENTAÇÃO DE PROCESSO LICITATÓRIO- PREGÃO

01	PORTARIA	S/N(*)	PÁGINA
02	PROJETO BÁSICO		
03	PESQUISA DE PREÇO NO MERCADO		
04	TABELA DE BLOQUEIO		
05	AUTORIZAÇÃO DA LICITAÇÃO		
06	CI'S DAS ÁREAS TÉCNICAS E JURIDICAS		
07	EDITAL E ANEXOS CHANCELADOS PELO DEJUR		
08	COMPROVANTE/PUBLICAÇÃO NO DOU		
09	RECIBOS REFERENTES ÀS RETIRADAS DO EDITAL DE LICITAÇÃO		
10	RESPOSTAS SOBRE O EDITAL DE LICITAÇÃO		
11	IMPUGNAÇÃO AOS TERMOS DO ART12 E DECRETO 3.555/00, DECISÃO E CONHECIMENTO À IMPUGNANTE (O AR DEVE CONSTAR NO PROCESSO		
12	CREDENCIAMENTO E DECLARAÇÃO		
13	PROPOSTAS ECONÔMICAS		
14	DOCUMENTOS DE HABILITAÇÃO		
15	ATA DE REUNIÃO DE ADJUDICAÇÃO DO PREGOEIRO		
16	RECURSOS		
17	ENVIO DOS RECURSOS PARA IMPUGNAÇÃO/DEJUR		
18	DECISÃO DOS RECURSOS		
19	REABERTURA DO PREGÃO: SE O RECURSO FOR PROCEDENTE		
20	DOCUMENTOS DE HABILITAÇÃO DO VENCEDOR DA		
21	ATA DE REUNIÃO E ATO DE ADJUDICAÇÃO DO PREGOEIRO		
22	RECURSOS		
23	IMPUGNAÇÃO/DEJUR		
24	RELATÓRIO HOMOLOGAÇÃO		
25	PUBLICAÇÃO NO DOU		
26	TERMO DE CONTRATO		
27	DEMAIS DOCUMENTOS		
28	PAGINAÇÃO DO PROCESSO		

OBS: - (*) S- APLICÁVEL
N- NÃO APLICÁVEL

CORREIOS

Diretoria de Administração
Departamento de Contratação e Administração de Material - DECAM
Comissão Permanente de Licitação – CPL/AC

PREGÃO 050/2003
AQUISIÇÃO DE EQUIPAMENTOS DE INFORMÁTICA PARA OS CCD'S
TIPO: Menor Preço

INÍCIO : 01/07/2003
ABERTURA:24/07/2003

ORIGEM:
CI/CAS/DCON/DECAM-4.544/2003

CLASSIFICAÇÃO ORÇAMENTÁRIA: 00.8.00/7.03

REQUISITANTE: DECAM

DESTINATÁRIO: BSB E SPM

VALOR ESTIMADO: R$ 145.713.124,35

VALOR ADJUCADO:

PUBLICAÇÃO DO RESULTADO:

QUANTIDADE: 162

DESENVOLVIMENTO

Na CPL elaborando edital.

RECURSO:

PRAZO TOTAL:

CORREIOS

Protocolo

7535

De: PREGOEIRA/AC

Ao: CHEFE DO DECAM

CI / CPL/AC - 1045/2003

Ref.: Pregão 050/2003 - CPL/AC

Assunto: Encaminha processo

Brasília, 01 de outubro de 2003.

Encaminhamos a V.Sª., em anexo, o processo licitatório sob referência, constituído de 42 pastas, cujo objeto é a locação de 162 equipamentos de informática incluinda assistência técnica e treinamento, para gestão desse Órgão.

Posteriormente, encaminharemos o original da planilha de custo de formação do preço com os ajustes de arredondamento necessário.

Informamos que as pastas de nºs **02, 10 e 11** estão no **DERCO**, sob análise, com os empregados **Joseph e Hugo Viana, ramais 2112 e 2886**.

Atenciosamente,

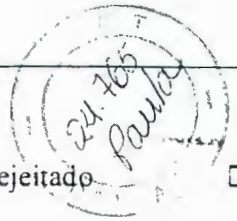
MARTA MARIA COELHO
Pregoeira/AC

ANEXO: Processo do Pregão 050/2003
C/C: DERCO e DPROD

FCAR/fcar

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls: 1025
3685
Doc:

CORREIOS



☐ Aprovado ☐ Retirado ☐ Rejeitado ☐ Em Vistas

IDENTIFICAÇÃO: Relatório/DITEC-028/2003

REUNIÃO: REDIR-030/2003 DATA REUNIÃO: 30/07/2003

ASSUNTO: Homologação do Pregão-050/2003-CPL/AC - Locação e instalação de equipamentos de informática destinados aos Centros Corporativos de Dados da ECT.

I. PROPOSTA

Homologar o Pregão 050/2003 – CPL/AC, no valor global de R$ 106.036.869,19 (cento e seis milhões e trinta e seis mil e oitocentos e sessenta e nove reais e dezenove centavos), com adjudicação a empresa HEWLETT PACKARD BRASIL LTDA., cujo objeto é a locação e instalação de 162 (cento e sessenta e dois) equipamentos de informática – novos de fábrica, incluindo a configuração, o treinamento, a assistência técnica e a garantia, destinados aos Centros Corporativos de Dados da ECT, localizados nas cidades de Brasília e São Paulo, pelo período de 48 (quarenta e oito) meses.

APLICAÇÃO/META: Expandir os Centros Corporativos Dados – CCD's da ECT localizados nas cidades de Brasília e São Paulo.

ÓRGÃO REQUISITANTE: DPROD/DITEC (CI/GAB/DPROD - 615, 552 e 493/2003).

EMPRESA A CONTRATAR: HEWLETT PACKARD BRASIL LTDA.

OBJETO: Locação e instalação de 162 (cento e sessenta e dois) equipamentos de informática – novos de fábrica, incluindo: a configuração, o treinamento, a assistência técnica e a garantia, destinados aos CCD's da ECT localizados nas cidades de Brasília e São Paulo.

VALOR CONTRATUAL: R$ 106.036.869.19 (cento e seis milhões e trinta e seis mil e oitocentos e sessenta e nove reais e dezenove centavos). sendo o preço global da locação pelo período de 48 (quarenta e oito) meses de R$ 104.986.999.20. acrescido de R$ 1.049.869.99 (um milhão e quarenta e nove mil oitocentos e sessenta e nove reais e noventa e nove centavos), correspondente a 1% (um por cento) do valor total da locação. relativo à apresentação do cronograma de trabalho. condicionado à instalação dos recursos necessários para o perfeito funcionamento dos equipamentos locados.

PRAZO DE VIGÊNCIA: 48 meses a contar da data de emissão do Termo de Aceitação da Fase III (Aceitação final dos equipamentos).

PERIODICIDADE DE REAJUSTE: Anual.

FORMA DE REAJUSTE: Mediante repactuação dos preços, tendo por parâmetros básicos a qualidade dos serviços e os preços vigentes no mercado, conforme orientações expedidas pelo Poder Público (Resolução nº 010/96 de 08/10/96), emitida pelo Conselho de Controle de Empresas Estatais - CCE.

FORMA DE PAGAMENTO: Os pagamentos serão efetuados, mediante apresentação de Nota Fiscal/Fatura devidamente atestada pela ECT, conforme a seguir:

- ✓ R$ 1.049.869.99, referente a 1% do valor total da locação, pago em parcela única. no 15º dia útil após a data de emissão do Termo de Aceitação da Fase I (Apresentação do cronograma de trabalho, condicionado à instalação dos recursos necessários para o perfeito funcionamento dos equipamentos locados);
- ✓ R$ 2.187.229.15 mensais, referentes aos 48 (quarenta e oito) meses de aluguel. no 15º dia útil do mês subseqüente ao da prestação dos serviços, após a emissão do Termo de Aceitação da Fase III (Aceitação final dos equipamentos).

CONTA/ATIVIDADE: 07.03/00.8.00

AUTORIZAÇÃO DE BLOQUEIO: DORC/DEORC- 70329/2003

II. INDICATIVO DE COMPETÊNCIA

Diretoria da ECT. conforme Relatório/PR-067/2003, da 15º REDIR, de 16/04/2003.

III. PROCESSO LICITATÓRIO

24 fls 103 Paula

Modalidade da Licitação: Pregão

- retiraram o edital: 79. sendo 10 pelo sistema impresso
  69 pelo sistema magnético. através da internet
- participaram da licitação: 04
- classificadas a dar lances: 03
- desclassificadas do processo: 00
- inabilitadas: 00

Propostas Classificadas:

Locação e instalação de 162 equipamentos de informática:

EMPRESAS	(*) VALOR TOTAL (R$)		POSIÇÃO (%)
	PROPOSTA ESCRITA	COM BASE MELHOR LANCE E/OU PROPOSTA	
HP BRASIL	**121.003.668,48**	**104.986.999,20**	**100,00**
ITAUTEC	194.794.890.72	105.950.000.00	100,92
NEC DO BRASIL	213.167.991.84	-	
Valor de referência (**)	145.713.124,35		138,79

(*) Valor da locação excluído o 1%. relativo a apresentação do cronograma de trabalho
(**) Valor de Referência fornecido pelo DECAM com base na média dos valores da pesquisa de mercado

IV. ÚLTIMAS AQUISIÇÕES

O contrato anterior contempla a locação de uma Solução Integrada de 2 (dois) Centros Corporativos de Dados, com tecnologia e equipamentos distintos (defasagem tecnológica) dos contratados através deste Pregão, portanto não existem parâmetros que permitam a comparação.

V. HISTÓRICO DO PROCESSO LICITATÓRIO

Recebido na CPL para licitar (expediente inicial)	02/07/2003
Data da veiculação do edital em D.O.U.	07/07/2003
Aviso de prorrogação – veiculação no D.O.U.	10/07/2003
Reunião de abertura	24/07/2003
Recebido na DITEC para Homologação	25/07/2003

VI. FUNDAMENTAÇÃO LEGAL

24762 Paulo

- Lei n.º 8.666/1993;
- Lei n.º 10.520/2002;
- Decreto n.º 3.555/2000;
- Decreto n.º 3.784/2001;
- MANLIC (Manual de Licitação e Contratação).

VII. INFORMAÇÕES COMPLEMENTARES

Consoante às orientações emanadas na CI/CAS/DECAM-4.544/2003, a CPL/AC deflagrou a presente licitação, tipo menor preço, objetivando a locação e instalação de 162 (cento e sessenta e dois) equipamentos de informática – novos de fábrica, incluindo: a configuração, o treinamento, a assistência técnica e a garantia, destinados aos CCD's da ECT localizados nas cidades de Brasília e São Paulo, conforme a seguir:

Descrição do item	Quantidade
Servidor INTEL tipo 01	21
Servidor INTEL tipo 02	35
Servidor INTEL tipo 03	51
Servidor RISC 01	11
Switch tipo 01	04
Switch tipo 02	06
Switch tipo 03	06
Switch tipo 04	12
Switch tipo 05	02
Roteador tipo 01	02
Roteador tipo 02	02
Unidade de Backup robotizado	02
Servidor de segurança lógica tipo 01	04
Servidor de segurança lógica tipo 02	02
Servidor para detecção de intrusão	02

24761
Paula

A presente contratação visa Expandir os Centros Corporativos Dados – CCD's visando obter condições para o pleno funcionamento de sistemas, atendendo às necessidades de equipamentos com relação aos seguintes ambientes: ERP, CHT, CHR, Banco Postal, SARA, serviços de rede, sistemas corporativos, etc.

Em 24/07 03 foi realizado o Pregão 050/2003 CPL/AC, com a participação de 04 (quatro) empresas, a saber: HP BRASIL, ITAUTEC, NEC DO BRASIL e COBRA. Após análise das propostas, foram classificadas para dar lance as empresas HP, Itautec e Nec, sendo vencedora do Pregão a empresa HEWLETT PACKARD BRASIL LTDA., com o preço global da locação pelo período de 48 (quarenta e oito) meses de R$ 104.987.000.00 (cento e quatro milhões e novecentos e oitenta e sete mil reais), perfazendo o valor total da proposta de R$ 106.036.870,00 (cento e seis milhões e trinta e seis mil e oitocentos e setenta reais) já incluso o valor de R$ 1.049.870,00 (um milhão e quarenta e nove mil e oitocentos e setenta reais), correspondente a 1% (um por cento) do valor total da locação.

Conforme previsto em Ata da Reunião de Licitação (28/07/2003), a adjudicatária teria que apresentar a nova proposta com os preços unitários de cada item da planilha ajustados, de acordo com o valor total, tendo assim procedido, porém por questão de arredondamento o valor total adjudicado sofreu uma alteração de R$ 0,81 (oitenta e um centavos) a menor.

Diante do exposto, submetemos o assunto à apreciação desse Colegiado, propondo a homologação da adjudicação à empresa HEWLETT PACKARD BRASIL LTDA., com o preço global da locação pelo período de 48 meses de R$ 104.986.999,20 (cento e quatro milhões novecentos e oitenta e seis mil novecentos e noventa e nove reais e vinte centavos), perfazendo o valor total da proposta de R$ 106.036.869,19 (cento e seis milhões e trinta e seis mil e oitocentos e sessenta e nove reais e dezenove centavos), já incluso o valor de R$ 1.049.869,99 (um milhão e quarenta e nove mil e oitocentos e sessenta e nove reais e noventa e nove centavos) correspondente a 1% do valor total da locação.

VIII. ANEXOS

1. CI/GAB/DPROD-615, 552 e 493/2003;
2. Autorização Abertura da Licitação/Parecer CACE-005/2003;

3. Ata da Sessão:
4. Ata-2 de Reunião de Licitação:
5. Autorização Bloqueio: DORC/DEORC-70329/2003.

24760 Paula

Eduardo Medeiros de Morais
Diretor de Tecnologia e de Infra-Estrutura

EMPRESA BRASILEIRA DE CORREIOS E TELÉGRAFOS

ÁREA RESERVADA AO PROTOCOLO

24 751 Paula

De: PRT/DITEC-012/2003

Ao: COMITÊ DE AVALIAÇÃO DAS CONTRATAÇÕES ESTRATÉGICAS

CI/GAB/DPROD - 615 / 2003

Ref.: CI/GAB/DPROD-493/2003 de 15/05/2003

Assunto: Expansão dos CCD's.

~~RQS nº 03/2005 - CN~~
CPMI - CORREIOS
Fls: 1032
Doc: 3685

Brasília. 13 de junho de 2003.

Em retificação à CI em referência. solicitamos considerar as seguintes alterações. tendo em vista que em 15 de maio. ainda não possuíamos as informações sobre a modalidade de aluguel e a totalidade da pesquisa de preços.

A modalidade de aluguel com opção de compra, segundo parecer jurídico, é caracterizada como arrendamento mercantil (leasing) e este tipo de operação esta contingenciada pelo Banco Central em R$ 1 bi ao ano, conforme podemos observar na resolução em anexo, em contato com o Banco Central fomos informados que os valores para o ano de 2003 e 2004 já estão comprometido, desta forma não havendo saldo disponível para que qualquer outro órgão publico da administração direta ou indireta obtenha autorização para contratar produtos ou serviços nesta modalidade, não restando outra alternativa a não ser a contratação pelo regime de aluguel. desta forma deve ser alterado o item objeto conforme a seguir:

> **Item Objeto**: Contratação, **em regime de aluguel** de 162 (cento e sessenta e dois) equipamentos de informática, incluindo: o Fornecimento, a Instalação, a Configuração, o Treinamento, a Assistência Técnica e a Garantia, destinados aos Centros Corporativos de Dados da ECT, localizados nas cidades de Brasília e São Paulo. Caberá à CONTRATADA fornecer, garantir compatibilidade e portabilidade, bem como instalar, configurar, dar assistência técnica aos equipamentos fornecidos e treinar a equipe técnica da CONTRATANTE, durante 48 (quarenta e oito) meses.

Os valores iniciais constante na documentação enviada a esse Comitê foram levantados de forma extra oficial baseados em informações constantes em sites ou documentos comerciais das empresas, sendo que os mesmo eram referentes somente a aquisição de equipamentos, os quais totalizavam o valor de R$ 127 mi, desta forma não consideravam os serviços de Instalação, a Configuração, o Treinamento e a Assistência Técnica. os quais fazem parte do objeto desta contratação.

A pesquisa de mercado realizada pelo Decam, indica o valor de aquisição da solução completa em torno de R$ 130 mi, entretanto, devido a necessidade de alteração da modalidade de contratação para aluguel o valor global obtido foi de R$ 190 mi,

JAAP/jaap

2458 Laura

segundo informações da area financeira se o valor global for remetido para o valor presente o mesmo seria algo em torno de R$ 80 mi. indicando ser vantajoso financeiramente a contratação por meio de aluguel.

A alteração na modalidade de contratação, a qual não nos permite ficar com os bens no final do contrato, nos leva a retirar do conjunto das soluções os equipamentos de armazenamento (storage), pois nestes equipamentos estarão armazenadas todas as informações dos sistemas corporativos da Empresa. Devido ao caráter estratégico destes equipamentos é importante que os mesmos devam ser adquiridos, e não locados, o que nos permitirá que ao final do contrato de aluguel dos equipamentos da solução possamos manter as informações dos sistemas corporativos em equipamentos próprios no nosso ambiente de produção.

Desta forma, os valores de locação obtidos na pesquisa de mercado, em anexo, que montam a ordem dos R$ 190 mi, foram reduzidos para R$ 141 mi com a retirada dos equipamentos de armazenamento, mostrando que na solução de aluguel estes equipamentos tem um custo global de R$ 49 mi.

O custo de aquisição dos equipamentos de armazenamento é da ordem de R$22 mi, o que alteraria o valor de aquisição da solução inicial para R$ 108 mi. A retirada destes equipamentos da contratação sob a modalidade de aluguel é necessário devido a importância do mesmo dentro do caráter estratégico da solução, o que nos indica que estes equipamentos deveram ser adquirido em um outro processo licitatório.

Colocamo-nos a disposição para maiores esclarecimentos e / ou dirimir quaisquer duvidas que por ventura possam surgir.

Atenciosamente,

Edilberto Nerry Petry
Coordenador GT Ditec-012/03

Waldimir Rosa da Silva
Chefe do DPROD

De Acordo:

Eduardo Medeiros de Morais
DITEC

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls: 1033
3685
Doc:

ANEXOS: Parecer Jurídico 458/2003. Resolução BACEN 2.827/2001. Pesquisa de Mercado realizada pelo Decam e Parecer do Deorc DAEF-1488/2003.

JAAP/jaap

EMPRESA BRASILEIRA DE CORREIOS E TELÉGRAFOS

ÁREA RESERVADA AO PROTOCOLO

24754 Paula

De: GRUPO DE TRABALHO – PRT/DITEC-012/2003

Ao: COMITÊ DE AVALIAÇÃO DAS CONTRATAÇÕES ESTRATÉGICAS

CI/GAB/DPROD- 552 / 2003

Ref.: CI/GAB/DPROD-493/2003

Assunto: Expansão dos CCD's.

Brasília, 29 de maio de 2003.

Em aditamento à CI em referência, de modo a complementar as informações que possibilitem a análise por parte desse Comitê, ressaltamos os tópicos a seguir:

3. **Avaliação de Impacto:**

- **Tecnológico:**

  - A contingência do Banco Postal será implementada na modalidade "off line", até que a solução de site back-up seja concluída, quando será possível total redundância dos ambientes de forma "on line".

  - As licenças para softwares de apoio (Websphere, banco de dados Oracle e InfoPrint) estarão sendo adquiridas mediante contratos em separado, estimamos um investimento de aproximadamente R$ 10.000.000,00.

  - A comparação dos equipamentos contratados com a IBM, pelo contrato 10.669/01, torna-se inviável, visto que a tecnologia atual é muito diferente daquela, onde não existia o conceito de particionamento lógico dos servidores e os equipamentos apresentam desempenho muito inferior (< 50 %) ao dos novos.

  - Os atuais equipamentos dos CCD representam um poder de processamento da ordem de 700.000 TPM-C. Após a contratação proposta, estaremos adicionando 1.800.000 TPM-C a essa capacidade.

- **Recursos Humanos:** Considerar as necessidades apontadas no Business Plan (item 6.1) como quantitativo ideal. Porém, o projeto não fica inviabilizado pelo não atendimento total de imediato.

4. **Informações Complementares:**

JAAP jaap

Como a atual demanda representará, no mínimo, 70 % do total de recursos a serem contratados, 20 % devem ser reservados por recomendação do fabricante e, apenas 10 % , destinados para futuras demandas;

Quanto ao fracionamento torna-se inviável, tendo em vista que estamos contratando uma solução e todo esse conjunto deverá ser integrado aos recursos já existentes, bem como aos novos equipamentos.

Com relação à opção quanto a modalidade de contratação, não nos restou outra alternativa senão a de aluguel ou aquisição via arrendamento mercantil, tendo em vista a limitação orçamentária de investimento para 2003.

Aproveitamos para ressaltar a necessidade imediata de expansão dos dois Centros Corporativos de Dados, sob pena de não cumprimento aos cronogramas de implantação dos sistemas corporativos para o ano de 2003.

O bloqueio orçamentário foi aprovado e liberado pela área financeira restando, apenas, a emissão da TDC.

Atenciosamente,

Edilberto Nerry Petry
Consultor de Diretoria

Waldimir Rosa da Silva
Chefe do DPROD

De Acordo:

Eduardo Medeiros de Morais
DITEC

C/Anexo: Business Plan – Expansão dos CCD's
Parecer Jurídico
Parecer Financeiro

JAAP jaap

EMPRESA BRASILEIRA DE CORREIOS E TELÉGRAFOS

24.755
Paula

De: DPROD/DITEC

Ao: COMITÊ DE AVALIAÇÃO DAS CONTRATAÇÕES ESTRATÉGICAS

CI/GAB/DPROD- 493 /2003

Ref.: PRT/PR-169/03

Assunto: Pregão – Expansão dos CCD's.

Brasília, 15 de maio de 2003.

Dando cumprimento ao contido na Portaria em referência, enviamos o processo de aquisição de novos recursos para os Centros Corporativos de Dados da ECT (Expansão dos CCD's) para análise desse Comitê, ressaltando os tópicos a seguir:

1. **Dados da Contratação**
   - **Modalidade:** Pregão.
   - **Objeto:** Contratação, em regime de aluguel com opção de compra, de **164 (cento e sessenta e quatro)** equipamentos de informática, incluindo: **o Fornecimento, a Instalação, a Configuração, o Treinamento, a Assistência Técnica e a Garantia**, destinados aos Centros Corporativos de Dados da ECT, localizados nas cidades de Brasília e São Paulo. Caberá à **CONTRATADA** fornecer, garantir compatibilidade e portabilidade, bem como instalar, configurar, dar assistência técnica aos equipamentos fornecidos e treinar a equipe técnica da **CONTRATANTE**, durante **48 (quarenta e oito)** meses após a aceitação final. O fornecimento deverá prever:
     - Preparação do ambiente de produção, provendo interoperabilidade com o ambiente já existente, relativamente aos itens: Rede TCP/IP, Segurança de Rede e Gerenciamento;
     - Migração dos dados do atual sistema de armazenamento (Storage IBM 2105 F20) para o sistema de armazenamento fornecido com o mínimo de impacto na produção dos sistemas;
     - Instalação e configuração dos produtos cotados;
     - Assistência Técnica, e
     - Treinamento.

   - **Valor Estimado**: Baseado em processo semelhante, cancelado por falta de orçamento, ocorrido em setembro/2002, estimamos um custo de R$2.670.000,00 / mês, no prazo de 48 (quarenta e oito) meses. Total: R$127.560.000,00.
   - **Classificação Orçamentária:** Conta 07.03 – Aluguel de equipamentos.

24 752 Paula

- **Justificativa da Contratação**: Com a referida expansão, estaremos atendendo as necessidades de equipamentos com relação aos seguintes ambientes:

  - ERP - Grupo I, Grupo II, Paralelo e Siebel;
  - CHT - Cluster de Banco de Dados e Recursos para o Gerenciamento da Impressão dos Telegramas – InfoPrint;
  - CHR - Adequação dos recursos do CHR (Cluster de Aplicação e Banco de Dados) e Ambiente de Desenvolvimento;
  - Banco Postal - Ambiente de Treinamento/Desenvolvimento;
  - SARA - Ambiente de Aplicação e BD (Cluster), Ambiente de Treinamento/ Desenvolvimento/Homologação;
  - Serviços de Rede (Centralização do Correio Eletrônico, Migração dos Domínios de Rede, Recursos para o Ambiente Internet e Intranet);
  - Sistemas Corporativos (CPF On Line, entre outros);
  - Infra-Estrutura dos CCDs (Segurança Lógica, Conectividade, Storage e Backup). Obter condições para o pleno funcionamento dos demais sistemas como, por exemplo, Equipamentos de Rede, Armazenamento de Dados, Backup Centralizado, Softwares, VPN, etc.

- **Situação Atual:** Conforme BUSINESS PLAN (anexo), item 1.2, página 3.

2. Informações Gerais:

- **Política Interna de contratação para o objeto a ser contratado:** É política da Empresa a contratação centralizada de servidores, como procedido na Concorrência 022/2000, cujo contrato 10.669/01 encontra-se em vigor, onde foram contratados 72 (setenta e dois) equipamentos para os CCDs, na modalidade aluguel por 48 (quarenta e oito) meses. porém, sem a opção de compra, o que provocará um impacto negativo ao término do contrato quando as máquinas serão devolvidas ao fornecedor.

- **Compatibilização da contratação com as Diretrizes do Plano Estratégico da ECT:** Atende ao item 3.4.6. Recomendações Estratégicas, alíneas a), b) e c) do tópico Rede de Atendimento do Plano Estratégico 2002 – 2005 da ECT. Adicionalmente, está em conformidade com o Plano Diretor de Tecnologia da Informação – PDTI, tópico 4.2 – Políticas e Diretrizes Estratégicas (página 13).

- **Viabilidade Técnica:** O projeto é totalmente compatível com os equipamentos existentes nos Centros Corporativos de Dados, sendo

24753 Paula

O atual contrato de aluguel com a IBM, 10.669/01, que engloba os equipamentos existentes nos CCD de Brasília e de São Paulo, representa um custo mensal de R$ 792.081,70 e encontra-se no 24º mês, tendo sido gastos, até o mês de maio/2003, R$ 20.487.347,70, correspondentes às mensalidades (R$19.009.960,80), ônus iniciais (R$ 891.129,75) e treinamento da equipe de operação e suporte (R$ 586.257,15).

5. Recomendações:

Como o atual processo deveria ter ocorrido ano passado, os prazos para a implantação de alguns projetos poderão sofrer impacto, visto o atraso decorrente do cancelamento, por falta de orçamento, ocorrido em setembro/2002.
Recomendamos, portanto, a máxima celeridade nos diversos passos para início do processo.

6. Conclusão:

Conforme o exposto, caso não ocorra a expansão dos recursos atualmente existentes nos CCDs, não haverá como garantir a implantação dos projetos citados na justificativa da contratação.

Atenciosamente,

Waldimir Rosa da Silva
Chefe do DPROD

De Acordo:

Eduardo Medeiros de Morais
DITEC

C/Anexo: Business Plan – Expansão dos CCD's

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls: 1038
3685
Doc:

JAAP/raap C:\Trabalho\CTCT_COMITE_ ...mado_CCD3.doc

CORREIOS

24.752 Paula

Continuação do PARECER/CACE-005/2003

Sr. Presidente.

Submeto à apreciação de V.Sa. a proposta de autorização de abertura da licitação para a locação de 162 equipamentos (servidores, roteadores e switch), no valor total estimado de R$ 145.713.124,35, conforme disposto neste Parecer. A proposta de autorização de abertura da licitação para a aquisição de 2 unidades de armazenamento (Storage) ocorrerá oportunamente, tendo em vista que aguardamos autorização dos órgãos governamentais de reformulação do orçamento de investimento já aprovada pela Diretoria da ECT.

Brasília 26 / 06 /2003.

Eduardo Medeiros de Morais
Diretor de Tecnologia e de Infra-Estrutura

Autorizo a abertura das licitações, conforme previsto neste Parecer.

Brasília 26 / 06 /2003.

Airton Langaro Dipp
Presidente da ECT

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls: 1030
3685
Doc:

24751
Paula

CORREIOS

PARECER/CACE-005/2003

Assunto: Solicitação de Abertura de Licitações para a Locação e Aquisição de Equipamentos para a Expansão dos Centros Corporativos de Dados de Brasília e de São Paulo.

Referência: ATA da 11ª Reunião do Comitê, de 24/06/2003. CI/GAB/DPROD-615/2003, 552/2003 e 493/2003.

1. **Dados da Contratação:**

= **Modalidades:** Pregões

⇒ **Objetos:**

a) Contratação, em regime de aluguel, de 162 (cento e sessenta e dois) equipamentos de informática, incluindo: fornecimento, instalação, configuração, treinamento, assistência técnica e garantia dos equipamentos (servidores, roteadores e switch), destinados aos Centros Corporativos de Dados da ECT, localizados nas cidades de Brasília e São Paulo, pelo período total de 48 (quarenta e oito) meses.

Tipo de Equipamento	Quantidade		
	CCD - BSB	CCD - SPM	Total
Servidos INTEL Tipo 1	14	7	21
Servidos INTEL Tipo 2	29	6	35
Servidos INTEL Tipo 3	27	24	51
Servidos RISC Tipo 1	8	3	11
SWITCH Tipo 1	2	2	4
SWITCH Tipo 2	4	2	6
SWITCH Tipo 3	4	2	6
SWITCH Tipo 4	8	4	12
SWITCH Tipo 5	1	1	2
Roteador Tipo 1	1	1	2
Roteador Tipo 2	2	0	2
Unidade de Backup Robotizado	1	1	2
Servidor de Segurança Lógica tipo 01	2	2	4
Servidor de Segurança Lógica tipo 02	1	1	2
Servidor para Detecção de Intrusão	1	1	2
Total			162

b) Aquisição de 2 (duas) unidades de armazenagem, com instalação, configuração, treinamento, assistência técnica e garantia pelo período total de 48 (quarenta e oito) meses, sendo uma unidade de 12,5 TB para o CCD de São Paulo e outra de 20 TB para o CCD de Brasília.

⇒ **Valores Estimados:**

- ✓ Aquisição das Unidades de Armazenagem (Storage): R$ 22.228.820,90;
- ✓ Locação dos 162 equipamentos (servidores, roteadores e switch): R$ 145.713.124,35.

⇒ **Classificação Orçamentária:**

- ✓ Atividade 00.8.00 - Conta 07.03
- ✓ Projeto: 17.1.06 – Conta 9.02

CORREIOS

24.150 Paula

⇒ **Justificativa da Contratação:** Obter condições para o pleno funcionamento dos demais sistemas como, por exemplo, Equipamentos de Rede, Armazenamento de Dados, Backup Centralizado, Softwares, VPN, etc. Com a referida expansão, o DPROD estará atendendo as necessidades de equipamentos com relação aos seguintes ambientes:

- ✓ ERP - Grupo I, Grupo II, Paralelo e Siebel;
- ✓ CHT - Cluster de Banco de Dados e Recursos para o Gerenciamento da Impressão dos Telegramas – InfoPrint;
- ✓ CHR - Adequação dos recursos do CHR (Cluster de Aplicação e Banco de Dados) e Ambiente de Desenvolvimento;
- ✓ Banco Postal - Ambiente de Treinamento/Desenvolvimento;
- ✓ SARA - Ambiente de Aplicação e BD (Cluster), Ambiente de Treinamento/ Desenvolvimento/Homologação;
- ✓ Serviços de Rede (Centralização do Correio Eletrônico, Migração dos Domínios de Rede, Recursos para ambientes Internet e Intranet);
- ✓ Sistemas Corporativos (CPF On Line, entre outros);
- ✓ Infra-Estrutura dos CCDs (Segurança Lógica, Conectividade, Storage e Backup).

⇒ **Situação Atual:**

O atual contrato de aluguel com a IBM, 10.669/01, que engloba os equipamentos existentes nos CCD de Brasília e de São Paulo, representa um custo mensal de R$ 792.081,70 e encontra-se no 24º mês, tendo sido gastos, até o mês de maio/2003, R$ 20.487.347,70, correspondentes às mensalidades (R$19.009.960,80), ônus iniciais (R$ 891.129,75) e treinamento da equipe de operação e suporte (R$ 586.257,15).

Com o término do projeto de implantação dos CCD´s e a gradativa entrada em produção dos sistemas previstos, também foram sendo implantados outros sistemas corporativos cujos projetos não previram recursos de hardware, tais como Correio Híbrido Reverso, IGRA, Vale Postal Internacional, Compras Eletrônicas, módulos adicionais do ERP (operacional e comercial), Automação da Rede de Atendimento - SARA, além da necessidade de ambientes de desenvolvimento, treinamento e homologação, estes projetos terminaram por esgotar rapidamente os equipamentos contratados.

Cabe ressaltar o crescimento dos serviços de rede (Correio Eletrônico, Internet, Intranet e FTP - transferência de arquivos), assim como o ambiente WEB institucional onde estão sendo incorporadas aplicações que automatizam processos internos e/ou externos (Help Desk, Falenosco, CPF online, Declaração de Isentos online entre outros) elevando a taxa de utilização dos serviços de Proxy e equipamentos da área de segurança (Firewalls, IDS e outros). O crescimento na utilização destes recursos e as demandas dos Novos Projetos apontam para uma atualização imediata na capacidade deste ambiente, evitando assim paralisarmos a implantação de novos projetos e de novos módulos em projetos já em produção.

ECT/DR/SP/GN
CPMI CORREIOS
Fls: 1041
3685
Doc.

2. Informações Gerais:

⇒ **Política interna de contratação para o objeto a ser contratado:** É política da Empresa a contratação centralizada de servidores, como procedido na Concorrência 022/2000, cujo contrato 10.669/01 encontra-se em vigor, onde foram contratados 72 (setenta e dois) equipamentos para os CCDs, na modalidade aluguel por 48 (quarenta e oito) meses.

⇒ **Compatibilização da contratação com as Diretrizes do Plano Estratégico da ECT:** Os equipamentos são essenciais para a viabilização de diversos projetos da Empresa, tais como Banco Postal, ERP, Correio Híbrido, Automação de Agências, dentre outros. Adicionalmente, está em conformidade com o Plano Diretor de Tecnologia da Informação – PDTI, tópico 4.2 – Políticas e Diretrizes Estratégicas (página 13).

CORREIOS

24 749 Paula

= **Viabilidade Técnica:** De acordo com as informações do DPROD, as especificações são compatíveis com os equipamentos existentes nos Centros Corporativos de Dados, sendo garantido o funcionamento dos produtos, conforme as especificações técnicas contidas no Business Plan.

= **Expectativa de Economicidade e Eficiência:**

Os atuais equipamentos dos CCD representam um poder de processamento da ordem de 700.000 TPM-C (Transações por minuto). Após a contratação proposta, estaremos adicionando 1.800.000 TPM-C a essa capacidade. Em termo de armazenagem, a nova contratação ampliará a capacidade de 7.5 TB para 40 TB.

Como a atual demanda representará, no mínimo, 70 % do total de recursos a serem contratados, 20 % devem ser reservados por recomendação dos fabricantes e, apenas 10%, destinados para futuras demandas. Ressalta-se que a demanda foi apurada a partir das informações disponibilizadas pelos Gestores dos Projetos.

Com a adoção da modalidade Pregão espera-se obter uma substancial redução dos custos ora estimados e uma redução dos prazos de realização dos processos licitatórios sem comprometer a qualidade da contratação pretendida. O DPROD informou que definiu especificações rígidas quanto à qualidade dos produtos e às condições de fornecimento.

3. Benefícios

⇒ **Operacional:** Permitirá a implantação do gerenciamento da impressão de telegramas e garantir o funcionamento do Correio Híbrido Reverso.
⇒ **Comercial:** Permitirá a implantação do SARA – Sistema de Automação da Rede de Agências e do ambiente de treinamento do Banco Postal
⇒ **Administrativo:** Permitirá a implantação dos módulos restantes do ERP e Data Warehouse.
⇒ **Tecnológico:** Permitirá realizar a centralização do correio eletrônico, a migração dos domínios da rede corporativa e bem como atender aos ambientes de Internet e Intranet. Além disso, permitirá atualizar a infra-estrutura dos CCDs (segurança lógica, conectividade, armazenamento de dado e backup).
⇒ **Recursos Humanos:** Permitirá a implantação dos módulos complementares do Populis (ERP).
⇒ **Financeiro:** Permitirá a implantação dos módulos restantes do ERP e Data Warehouse.

4. Impactos:

⇒ **Tecnológico:** As licenças para softwares de apoio (Websphere, banco de dados Oracle e InfoPrint) estarão sendo adquiridas mediante contratos em separado, estimando-se um investimento de aproximadamente R$ 10.000.000,00.
⇒ **Recursos Humanos:** Será necessária a complementação do efetivo do DPROD em 23 profissionais. Porém, segundo o DPROD, o não atendimento imediato não inviabiliza a proposta de ampliação dos CCDs.
⇒ **Financeiro:** As despesas com a locação dos equipamentos foram devidamente programadas no orçamento de 2003, 2004, 2005, 2006 e 2007, no valor total de R$ 125.040.000,00, sendo necessária a complementação do bloqueio no valor total de R$ 20.673.124,35. Além disso, para a compra das unidades de armazenagem será necessária a alocação de recursos da ordem de R$ 22.228.820,90, que não estão ainda previstos no Orçamento 2003 e nem 2004.

5. Informações Complementares:

REQUISIÇÃO Nº 03/2006 - CN - CPMI - CORREIOS
1042
Fls:
3685
Doc:

CORREIOS

24 KB Paula

= As atuais salas de segurança física (AC e SPM) possuem espaço físico suficiente para a instalação dos novos equipamentos, bem como a capacidade de refrigeração, no-break e proteção contra incêndio. As alterações necessárias nos quadros elétricos e cabeamento estão sendo contratadas junto com os equipamentos.

= Segundo a área técnica, as aplicações críticas do Banco Postal, do SARA e do ERP podem ser executadas em equipamentos que não são IBM, com exceção do SRO que será instalado nas máquinas desocupadas pelo ERP.

= A análise do Comitê contemplou tão somente os aspectos de caráter geral e conceitual da contratação proposta, não se detendo na avaliação de especificações técnicas e condições administrativas e operacionais vinculadas à execução dos serviços e dos fornecimentos, cuja formulação está sob a responsabilidade da Área Técnica e da Comissão de Licitação.

6. Considerações Gerais:

Inicialmente, o DPROD apresentou proposta de contratação dos 164 equipamentos, mediante locação com a opção de compra, descartando qualquer possibilidade de aquisição dos bens, tendo em vista as limitações orçamentárias de investimento para 2003, conforme disposto nas CI/GAB/DPROD-493/2003, de 15/05/2003 e CI/GAB/DPROD-552/2003, de 29/05/2002.

Considerando dúvidas manifestadas pelo Comitê em relação à aplicação prática deste tipo de contratação, o DPROD, em 30/05/2003, submeteu o assunto ao DEJUR, que por meio da NOTA JURÍDICA DEJUR/DJTEC-458/2003, de 10/06/2003, informou o seguinte:

a) O sistema de locação com a opção de compra nada mais é do que um típico contrato de leasing, também conhecido por arrendamento mercantil. Segundo o DEJUR é possível a contratação de solução de informática por contrato de arrendamento mercantil, conforme Nota Jurídica DEJUR/DJTEC-288/2003.

b) É possível inserir também num contrato de locação a doação não compulsória dos equipamentos por parte da Locadora.

c) Se constatado que a devolução dos equipamentos, no final do contrato de locação, redundará em prejuízos, poderá a ECT, se justificado tecnicamente, adquirir os equipamentos por inexigibilidade de licitação.

Com base nesse posicionamento e considerando as informações obtidas junto ao Banco Central em relação às normas vigentes e aos limites de créditos para a autorização de realização de operações de leasing, que impedem no momento a adoção desta modalidade de contratação por parte da ECT, o DPROD, por meio da CI/ASS/DPROD-615/2003, de 13/06/2003, descartou a possibilidade de realização do processo de locação com opção de compra e retificou a sua proposta inicial, desdobrando o processo em duas licitações distintas: uma para a locação dos 162 equipamentos, pelo período de 48 meses, e outra para a aquisição das 2 Unidades de Armazenamento do Dados

Este desdobramento, segundo o DPROD, foi determinado a partir da modificação da modalidade de contratação, que não permitirá, em princípio, permanecer com os equipamentos após o encerramento da vigência do contrato. No caso das unidades de armazenamento a sua aquisição é estratégica para a ECT, pois permitirá que, ao término da locação dos demais equipamentos, sejam preservadas todas as informações dos sistemas corporativos em ambientes da própria Empresa.

Além da alteração da modalidade de contratação, houve modificações dos preços estimados em relação ao anteriormente informado, considerando os novos valores obtidos a partir de pesquisa

CORREIOS

de mercado, realizada em maio/junho-2003. O valor total da locação de todos os equipamentos passou de R$ 127.560.00.00 para RS 194.873.688.00. Na pesquisa realizada obteve-se também os preços de aquisição dos bens, cujo menor foi de RS 130.757.770.00.

Empresas	Aquisição	Locação			
HP	130.757.770,00	4.259.981,50	48	204.479.112,00	
IBM	147.000.000,00	6.210.000,00	48	298.080.000,00	
POLICENTRO	150.000.000,00	6.225.345,00	48	298.816.560,00	
COBRA	Não opera com venda	3.964.684,00	48	190.304.832,00	
		2.869.001,00	6	17.214.006,00	190.584.210,00
		4.127.862,00	42	173.370.204,00	
		2.869.001,00	12	34.428.012,00	194.177.004,00
		4.437.472,00	36	159.748.992,00	
		2.869.001,00	6	17.214.006,00	194.873.688,00
		3.229.441,00	12	38.753.292,00	
		4.630.213,00	30	138.906.390,00	

Com a retirada das unidades de armazenamento do processo de locação, os novos valores estimados de locação dos 162 equipamentos passaram a ser os seguintes:

Alternativa	Valor Mensal	Quantidade de Parcelas	Valor Total	
1	2.942.192,00	48	141.225.215,83	
2	2.129.085,64	6	12.774.513,85	141.432.542,24
	3.063.286,39	42	128.658.028,39	
3	2.129.085,64	12	25.549.027,71	144.098.754,67
	3.293.047,97	36	118.549.726,96	
4	2.129.085,64	6	12.774.513,85	145.713.124,35
	2.396.568,17	12	28.758.817,99	
	3.472.659,75	30	104.179.792,50	

A valor da aquisição das unidades de armazenamento, orçado pela HP, foi de R$ 22.220.820,90

Ressalta-se a necessidade de serem definidos no Edital o quantitativo de parcelas de locação e, se for o caso, os percentuais correspondentes a cada parcela, considerando o limite da vigência contratual de 48 meses e os prazos de instalação e aceitação dos equipamentos.

7. Conclusão:

Diante do exposto, somos de parecer favorável ao desencadeamento das licitações em tela, conforme proposto pelo DPROD/DITEC, ressaltando, no entanto, a necessidade de ajuste do bloqueio orçamentário para a locação dos equipamentos, bem como a emissão de bloqueio específico para a aquisição das Unidades de Armazenamento (Storage).

Brasília, 24 de junho de 2003.

Marcos Gomes da Silva
Coordenador do Comitê

CORREIOS

Comissão Permanente de Licitação da Administração Central - CPL/AC

ATA DE REUNIÃO DE LICITAÇÃO
PREGÃO N.º 050/2003 - CPL/AC

OBJETO: Locação e instalação de 162 equipamentos de informática – novos de fábrica, incluindo: a configuração, o treinamento, assistência técnica e a garantia.

DIA/HORA: 24/07/2003 das 09:00 à 01:00 hora do dia 25/07/2003.

ASSUNTO: Esta Sessão destinou-se a abertura do Pregão n.º 050/2003-CPL/AC objetivando a obtenção da proposta mais vantajosa para a Administração, por meio de lances verbais disputados entre as licitantes. Foram recebidos e abertos os envelopes das propostas econômicas e o envelope de habilitação da firma vencedora.

LOCAL: Salão Nobre, localizado no SBN, Quadra 01, Bloco "A" - 1º sobreloja, do Ed. Sede da ECT, em Brasília/DF.

QUANTIDADE DE EDITAIS RETIRADOS: Foram retirados 79 (setenta e nove) exemplares do Edital, sendo 10 (dez) através do sistema impresso e 69 (sessenta e nove) através do sistema magnético, via Internet.

CREDENCIADOS: Compareceram à Sessão 04 (quatro) empresas relacionadas nesta ata.

ABERTURA DAS PROPOSTAS ECONÔMICAS: Após o credenciamento das participantes, procedeu-se a abertura e análise dos envelopes das propostas econômicas. Os preços unitários e totais cotados foram lidos para que os presentes tomassem conhecimento, conforme discriminado a seguir:

1-A) 21 SERVIDORES INTEL TIPO 01; **1-B)** 35 SERVIDORES INTEL TIPO 02; **1-C)** 51 SERVIDORES INTEL TIPO 03; **1-D)** 11 SERVIDORES RISC TIPO 01; **1-E)** 4 SWITCHES TIPO 01; **1-F)** 6 SWITCHES TIPO 02; **1G)** 6 SWITCHES TIPO 03; **1-H)** 12 SWITCHES TIPO 04; **1-I)** 2 SWITCHES TIPO 05; **1-J)** 2 ROTEADORES TIPO 01; **1-L)** 2 ROTEADORES TIPO 02; **1-M)** 2 UNIDADES DE BACKUP ROBOTIZADO; **1-N)** 4 SERVIDORES DE SEGURANÇA LOGICA TIPO 01;**1-O)** 2 SERVIDORES DE SEGURANÇA LÓGICA TIPO 02; e **1-P)** 2 SERVIDORES PARA DETECÇÃO DE INTRUSÃO:

EMPRESA	DESCRIÇÃO DO ITEM	QTDE.	PREÇO UNITÁRIO MENSAL (R$)	TOTAL MENSAL (R$)
ITAUTEC INFORMÁTICA S/A	1-A – SERV. TIPO 01	21	43.529,83	914.126,43
	1-B- SERV. TIPO 02	35	10.094,75	353.316,25
	1-C- SERV. TIPO 03	51	6.200,12	316.206,12
	1-D – SERV. RISC 01	11	97.694,37	1.074.638,07
	1-E SWITCH TIPO 01	04	46.753,28	187.013,12
	1-F - SWITCH TIPO2	06	2.718,84	16.313,04
	1-G - SWITCH TIPO3	06	44.414,25	266.485,50
	1-H - SWITCH TIPO4	12	9.105,27	109.263,24
	1-I- SWITCH TIPO5	02	24.131,98	48.263,96
	1-J – ROT. TIPO 01	02	12.854,11	25.708,22
	1-K – ROT. TIPO 02	02	3.927,21	7.854,42
	1-L –UNID. BACKUP	02	158.038,73	316.077,46
	1-M- SERV. LOG. T-01	04	93.318,65	373.274,60
	1-N - SERV. LOG. T-02	02	13.789,88	27.579,76
	1-O – SERV. DETEC.	02	11.053,35	22.106,70

CORREIOS

NEC DO BRASIL S/A	1-A – SERV. TIPO 01	21	23.326,86	489.864,06
	1-B- SERV. TIPO 02	35	11.632,43	407.135,05
	1-C- SERV. TIPO 03	51	2.891,10	147.446,10
	1-D – SERV. RISC 01	11	78.538,70	863.925,70
	1-E SWITCH TIPO 01	04	59.639,38	238.557,52
	1-F - SWITCH TIPO2	06	7.072,25	42.433,50
	1-G - SWITCH TIPO3	06	144.455,18	866.731,08
	1-H - SWITCH TIPO4	12	2.413,13	28.957,56
	1-I- SWITCH TIPO5	02	34.798,35	69.596,70
	1-J – ROT. TIPO 01	02	27.366,82	54.733,64
	1-K – ROT. TIPO 02	02	19.138,42	38.276,84
	1-L –UNID. BACKUP	02	431.962,84	863.925,68
	1-M- SERV. LOG. T-01	04	20.571,80	82.287,20
	1-N - SERV. LOG. T-02	02	23.558,04	47.116,08
	1-O – SERV. DETEC.	02	100.006,56	200.013,12
COBRA TECNOLOGIA S/A	1-A – SERV. TIPO 01	21	37.719,62	792.112,02
	1-B- SERV. TIPO 02	35	9.403,94	329.137,90
	1-C- SERV. TIPO 03	51	3.800,71	193.836,21
	1-D – SERV. RISC 01	11	136.006,10	1.496.067,10
	1-E SWITCH TIPO 01	04	130.189,25	520.757,00
	1-F - SWITCH TIPO2	06	3.517,50	21.105,00
	1-G - SWITCH TIPO3	06	45.107,38	270.644,28
	1-H - SWITCH TIPO4	12	49.726,75	596.721,00
	1-I- SWITCH TIPO5	02	4.387,50-	8.775,00
	1-J – ROT. TIPO 01	02	22.684,50	45.369,00
	1-K – ROT. TIPO 02	02	4.768,00	9.536,00
	1-L –UNID. BACKUP	02	96.057,50	192.115,00
	1-M- SERV. LOG. T-01	04	28.485,25	113.941,00
	1-N - SERV. LOG. T-02	02	14.600,50	29.201,00
	1-O – SERV. DETEC.	02	15.664,00	31.328,00
HP BRASIL LTDA.	1-A – SERV. TIPO 01	21	18.831,24	395.456,04
	1-B- SERV. TIPO 02	35	4.272,08	149.522,80
	1-C- SERV. TIPO 03	51	2.881,23	146.942,73
	1-D – SERV. RISC 01	11	110.328,55	1.213.614,05
	1-E SWITCH TIPO 01	04	25.586,63	102.346,52
	1-F - SWITCH TIPO2	06	627,90	3.767,40
	1-G - SWITCH TIPO3	06	14.668,73	88.012,38
	1-H - SWITCH TIPO4	12	4.079,65	48.955,80
	1-I- SWITCH TIPO5	02	2.829,07	5.658,14
	1-J – ROT. TIPO 01	02	8.602,54	17.205,08
	1-K – ROT. TIPO 02	02	2.263,04	4.526,08
	1-L –UNID. BACKUP	02	161.976,95	323.953,90
	1-M- SERV. LOG. T-01	04	2.405,68	9.622,72
	1-N - SERV. LOG. T-02	02	2.405,68	4.811,36
	1-O – SERV. DETEC.	02	3.257,38	6.514,76

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls: 1046
3685
Doc:

CORREIOS

Comissão Permanente de Licitação da Administração Central - CPL/AC

QUADRO RESUMO		
NOME DA EMPRESA	VALOR TOTAL MENSAL (R$)	VALOR GLOBAL (R$)
HP BRASIL	2.520.909,76	121.003.668,48
ITAUTEC	4.058.226,89	194.794.890,72
NEC DO BRASIL	4.440.999,83	213.167.991,84
COBRA	4.650.645,51	223.230.984,48

CLASSIFICACÃO DAS PROPOSTAS/RODADAS DE LANCES:

Todas as propostas foram analisadas tecnicamente pela equipe tecnica especialmente designada para este fim. As dúvidas surgidas das propostas das empresas **HP BRASIL, ITAUTEC, NEC DO BRASIL e COBRA** foram sanadas através de diligências junto às empresas, conforme DECLARAÇÕES em anexo, que farão parte das propostas das mesmas.

Após análise das propostas, foram classificadas e autorizadas a dar lances de acordo a alínea "d.2 " do edital as empresas relacionadas no quadro abaixo, iniciando as rodadas de lances com a empresa NEC DO BRASIL e terminando com a empresa **HP BRASIL** vencedora do certame com o preço total de R$ R$ 106.036.870,00 (cento e seis milhões e trinta e seis mil e oitocentos e setenta reais), incluído o 1% relativo a apresentação do cronograma de trabalho.

NOME DAS EMPRESAS	# VALOR TOTAL DA LOCAÇÃO (R$)	RODADAS DE LANCES			
		1ª	2ª	3ª	4ª
HP BRASIL	121.003.668,48	120.989.000,00	120.987.000,00	120.985.000,00	120.983.000,00
ITAUTEC	194.794.890,72	120.990.000,00	120.988.000,00	120.986.000,00	120.984.000,00
NEC DO BRASIL	213.167.991,84	*	*	*	*

= Valor total da locação excluído o 1%, relativo a apresentação do cronograma de trabalho
(*) Desistência de Lance

NOME DAS EMPRESAS	RODADAS DE LANCES				
	5ª	6ª	7ª	8ª	9ª
HP BRASIL	120.981.000,00	120.979.000,00	120.969.000,00	120.959.000,00	120.949.000,00
ITAUTEC	120.982.000,00	120.980.000,00	120.970.000,00	120.960.000,00	120.950.000,00

NOME DAS EMPRESAS	RODADAS DE LANCES				
	10ª	11	12ª	13ª	14ª
HP BRASIL	120.939.000,00	120.929.000,00	120.919.000,00	120.909.000,00	120.899.000,00
ITAUTEC	120.940.000,00	120.930.000,00	120.920.000,00	120.910.000,00	120.900.000,00

(*) Desistência de Lance

NOME DAS EMPRESAS	RODADAS DE LANCES				
	15ª	16ª	17ª	18ª	19ª
HP BRASIL	120.889.000,00	120.789.000,00	120.689.000,00	120.589.000,00	120.489.000,00
ITAUTEC	120.890.000,00	120.790.000,00	120.690.000,00	120.590.000,00	120.490.000,00

NOME DAS EMPRESAS	RODADAS DE LANCES				
	20ª	21ª	22ª	23ª	24ª
HP BRASIL	120.389.000,00	120.387.000,00	120.385.000,00	120.379.000,00	120.377.000,00
ITAUTEC	120.390.000,00	120.388.000,00	120.386.500,00	120.380.000,00	120.378.000,00

(*) Desistência de Lance

CORREIOS

Comissão Permanente de Licitação da Administração Central - CPLAC

NOME DAS EMPRESAS	RODADAS DE LANCES				
	25ª	26ª	27ª	28ª	29ª
HP BRASIL	120.375.000,00	120.373.000,00	120.371.000,00	120.369.000,00	120.367.000,00
ITAUTEC	120.376.000,00	120.374.000,00	120.372.000,00	120.370.000,00	120.368.000,00

(*) Desistência de Lance

NOME DAS EMPRESAS	RODADAS DE LANCES				
	30ª	31ª	32ª	33ª	34ª
HP BRASIL	120.265.000,00	120.164.000,00	120.063.000,00	119.787.000,00	119.487.000,00
ITAUTEC	120.266.000,00	120.165.000,00	120.064.000,00	120.000.000,00	119.687.000,00

(*) Desistência de Lance

NOME DAS EMPRESAS	RODADAS DE LANCES				
	35ª	36ª	37ª	38ª	39ª
HP BRASIL	118.887.000,00	118.786.000,00	118.749.000,00	118.693.000,00	118.637.000,00
ITAUTEC	119.387.000,00	118.787.000,00	118.750.000,00	118.700.000,00	118.650.000,00

NOME DAS EMPRESAS	RODADAS DE LANCES				
	40ª	41ª	42ª	43ª	44ª
HP BRASIL	118.587.000,00	118.547.000,00	118.539.000,00	118.227.000,00	117.987.000,00
ITAUTEC	118.600.000,00	118.550.000,00	118.540.000,00	118.530.000,00	118.220.000,00

NOME DAS EMPRESAS	RODADAS DE LANCES				
	45ª	46ª	47ª	48ª	49ª
HP BRASIL	117.587.000,00	117.287.000,00	116.867.000,00	116.757.000,00	116.657.000,00
ITAUTEC	117.980.000,00	117.580.000,00	117.280.000,00	116.860.000,00	116.750.000,00

NOME DAS EMPRESAS	RODADAS DE LANCES				
	50ª	51ª	52ª	53ª	54ª
HP BRASIL	116.557.000,00	116.457.000,00	116.357.000,00	116.257.000,00	116.157.000,00
ITAUTEC	116.650.000,00	116.550.000,00	116.450.000,00	116.350.000,00	116.200.000,00

NOME DAS EMPRESAS	RODADAS DE LANCES				
	55ª	56ª	57ª	58ª	59ª
HP BRASIL	116.057.000,00	115.497.000,00	114.997.000,00	114.757.000,00	114.557.000,00
ITAUTEC	116.100.000,00	116.000.000,00	115.450.000,00	114.950.000,00	114.700.000,00

NOME DAS EMPRESAS	RODADAS DE LANCES				
	60ª	61ª	62ª	63ª	64ª
HP BRASIL	114.487.000,00	114.387.000,00	114.287.000,00	114.247.000,00	114.241.000,00
ITAUTEC	114.500.000,00	114.450.000,00	114.350.000,00	114.250.000,00	114.242.000,00

NOME DAS EMPRESAS	RODADAS DE LANCES				
	65ª	66ª	67ª	68ª	69ª
HP BRASIL	114.229.000,00	114.219.000,00	114.209.000,00	114.199.000,00	113.987.000,00
ITAUTEC	114.230.000,00	114.220.000,00	114.210.000,00	114.200.000,00	114.100.000,00

NOME DAS EMPRESAS	RODADAS DE LANCES				
	70ª	71ª	72ª	73ª	74ª
HP BRASIL	113.949.000,00	113.899.000,00	113.487.000,00	113.387.000,00	113.287.000,00
ITAUTEC	113.950.000,00	113.900.000,00	113.850.000,00	113.150.000,00	113.380.000,00

CORREIOS

24742 Paulo

Comissão Permanente de Licitação da Administração Central - CPLAC

NOME DAS EMPRESAS	RODADAS DE LANCES				
	75ª	76ª	77ª	78ª	79ª
HP BRASIL	113.187.000,00	113.177.000,00	113.167.000,00	113.157.000,00	113.147.000,00
ITAUTEC	113.280.000,00	113.180.000,00	113.170.000,00	113.160.000,00	113.150.000,00

NOME DAS EMPRESAS	RODADAS DE LANCES				
	80ª	81ª	82ª	83ª	84ª
HP BRASIL	113.137.000,00	113.127.000,00	112.997.000,00	112.947.000,00	112.897.000,00
ITAUTEC	113.140.000,00	113.130.000,00	113.000.000,00	112.950.000,00	112.900.000,00

(*) Desistência de Lance

NOME DAS EMPRESAS	RODADAS DE LANCES				
	85ª	86ª	87ª	88ª	89ª
HP BRASIL	112.847.000,00	112.499.000,00	112.449.000,00	112.399.000,00	112.349.000,00
ITAUTEC	112.850.000,00	112.500.000,00	112.450.000,00	112.400.000,00	112.350.000,00

NOME DAS EMPRESAS	RODADAS DE LANCES				
	90ª	91ª	92ª	93ª	94ª
HP BRASIL	111.297.000,00	110.187.000,00	109.997.000,00	108.997.000,00	108.497.000,00
ITAUTEC	112.300.000,00	111.200.000,00	110.150.000,00	109.950.000,00	108.900.000,00

NOME DAS EMPRESAS	RODADAS DE LANCES				
	95ª	96ª	97ª	98ª	99ª
HP BRASIL	108.400.000,00	108.300.000,00	108.200.000,00	108.050.000,00	107.900.000,00
ITAUTEC	108.450.000,00	108.350.000,00	108.250.000,00	108.100.000,00	107.950.000,00

NOME DAS EMPRESAS	RODADAS DE LANCES				
	100ª	101ª	102ª	103ª	104ª
HP BRASIL	106.000.000,00	104.987.000,00			
ITAUTEC	107.500.000,00	105.950.000,00	*		

(*) Desistência de Lance

HABILITAÇÃO DA VENCEDORA: Após conferência da documentação da empresa **HEWLETT PACKARD BRASIL LTDA.** vencedora do Pregão, a mesma foi considerada habilitada. O envelope da empresa **ITAUTEC INFORMÁTICA S/A** ficará em poder da Pregoeira até a assinatura do Contrato. Os demais envelopes foram devolvidos a seus representantes presentes ao ato.

ADJUDICAÇÃO: A Pregoeira declarou vencedora a empresa **HEWLETT PACKARD BRASIL LTDA.**, CNPJ n.° 61.797.924/0001-55, com o preço global da locação pelo período de 48 (quarenta e oito) meses de R$ 104.987.000,00 (cento e quatro milhões e novecentos e oitenta e sete mil reais), perfazendo o valor total da proposta de R$ 106.036.870,00 (cento e seis milhões e trinta e seis mil e oitocentos e setenta reais), já incluso o valor de R$ 1.049.870,00 (um milhão e quarenta e nove mil e oitocentos e setenta reais), correspondente a 1% (um por cento) do valor total da locação, conforme previsto no Anexo 1-A, item 1.2. do Edital.

COMUNICADO: Fica acertado com o representante da empresa **HEWLETT PACKARD BRASIL LTDA.** que o mesmo deverá apresentar até o dia 28/07/2003 (segunda-feira) a proposta com os preços unitários ajustados de acordo com o último lance formulado.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls: 1049
3685
Doc:

CORREIOS

Comissão Permanente de Licitação da Administração Central - CPLAC

ENCERRAMENTO DA REUNIÃO: Nada mais havendo a tratar foi dada como encerrada a reunião, lavrada a presente Ata, que após lida e achada conforme, vai assinada pela Pregoeira e sua equipe e pelos representantes credenciados presentes ao ato.

Marta Maria Coelho
Pregoeira

24 741
Paula

Equipe de Apoio Administrativo:

Marise da Consolação Cerqueira Capella

Jeanne Roriz Suaden

Liana Aparecida de Araújo

Pedro Alberto da Silva Oliveira

Gilberto Ferreira do Amaral

Adriana Maria da Rocha Fonseca

Equipe de Apoio Técnico:

Edilberto Nery Petry

João Amaro Alves Pessanha

Hugo Viana

Roberto Stefan F. de Aguiar

Rogers Luis Cunha Pereira

Jefferson Colombo B. Xavier

Alexandre Pinto de Oliveira

Joseph Michel

Ruy Ney Muniz Barbosa

Daniel de Moreira Queiroga

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls: 1050
3685
Doc:

CORREIOS

Comissão Permanente de Licitação da Administração Central - CPL/AC

Representantes credenciados e as respectivas Empresas:

Empresa: ITAUTEC INFORMÁTICA S/A
Nome Representante: Jorge Ítalo Dimatteu Telles
Fone: (61) 323-3031 Fax: (61) 226-1251

Empresa: NEC DO BRASIL S/A
Nome Representante: Vair Doiche
Fone: (11) 6462-6190 Fax.: (11) 6462-7053

Empresa: HEWLETT PACKARD BRASIL LTDA.
Nome Representante: José Eduardo Pires do Rio Ribeiro
Fone: (11) 4197-8000 Fax: (11) 4197-8432

Empresa: COBRA TECNOLOGIA S/A
Nome Representante: Antonio Alves Ferreira
Fone: (21) 2442-8800 Fax.: (21) 2442-8814

CORREIOS

Comissão Permanente de Licitação da Administração Central - CPL/AC

24 / 39
Paula

ATA-2 DE REUNIÃO DE LICITAÇÃO
PREGÃO N.º -050/2003 - CPL/AC
RETIFICAÇÃO DE VALOR ADJUDICADO

Às 15:00 horas do dia 28 de julho do ano de 2003. na Sala de Reunião da Comissão Permanente de Licitação da Administração Central – CPL/AC. localizada no 4º Andar do Ed. Sede dos Correios. em Brasília. reuniu-se a Pregoeira. Marta Maria Coelho e sua Equipe de Apoio. para rever o valor adjudicado no Pregão n.º 050/2003. Consoante consignado na Ata da Sessão de abertura do Pregão em questão relativo à **locação e instalação de 162 equipamentos de informática – novos de fábrica, incluindo: a configuração, o treinamento. assistência técnica e a garantia,** foi adjudicado à empresa **HEWLETT PACKARD BRASIL LTDA.**, com o preço global da locação pelo período de 48 (quarenta e oito) meses de R$ 104.987.000,00 (cento e quatro milhões e novecentos e oitenta e sete mil reais), perfazendo o valor total da proposta de R$ 106.036.870,00 (cento e seis milhões e trinta e seis mil e oitocentos e setenta reais), já incluso o valor de R$ 1.049.870,00 (um milhão e quarenta e nove mil e oitocentos e setenta reais), correspondente a 1% (um por cento) do valor total da locação. conforme previsto no Anexo 1-A, item 1.2. do Edital. Ainda, consoante consignado na referida Ata. a adjudicatária teria que apresentar a nova proposta com os preços unitários de cada item da planilha ajustados, de acordo com o valor total, tendo assim procedido, porém por questão de arredondamento o valor total adjudicado sofreu uma alteração de R$ 0,81 (oitenta e um centavos) a menor, devendo pois o valor anteriormente adjudicado ser retificado de R$ **106.036.870,00** para **R$ 106.036.869,19** (cento e seis milhões, e trinta e seis mil e oitocentos e sessenta e nove reais e dezenove centavos), já incluso o valor de R$ 1.049.869,99 (um milhão e quarenta e nove mil e oitocentos e sessenta e nove reais e noventa e nove centavos), correspondente a 1% (um por cento) do valor total da locação. conforme previsto no Anexo 1-A, item 1.2. do Edital.

ENCERRAMENTO DA REUNIÃO: Nada mais havendo a tratar foi dada como encerrada a reunião. lavrada a presente Ata. que após lida e achada conforme. vai assinada pelo Pregoeiro e sua equipe presente ao ato.

Marta Maria Coelho
Pregoeira

Equipe de Apoio

Cláudio Nunes Barbosa

Pedro Alberto da Silva Oliveira

Marise da Consolação Cerqueira Capella

João Batista Vieira de Carvalho

RQS nº 03/2003 - CN - CPMI - CORREIOS
1052
Fls:
3685
Doc:

2473
Paula

CORREIOS

BLOQUEIO	EMITENTE	NÚMERO	DATA
	DORC/DEORC	70329	30/07/2003

GESTOR	DATA DA CONFIRMAÇAO	DEPENDENCIA-SOLICITANTE
DITEC	29/07/2003	01 Administração Central

PROJETO/ATIVIDADE
00.8.00 INFRA-ESTRUTURA

CONTA
800.07.03.0000 ALUGUEL DE EQUIPAMENTOS DE INFORMATICA

SOLICITANTE - No - DATA DA SOLICITAÇAO	REFERENCIA	TOTAL - R$
DITEC 3264 29/07/2003	3252	106.036.862,00

CRONOGRAMA DE EXECUÇÃO	MÊS	VALOR - R$	
2003			**5.424.328,00**
	10	1.049.870,00	
	11	2.187.229,00	
	12	2.187.229,00	
2004			**26.246.748.00**
	01	2.187.229,00	
	02	2.187.229,00	
	03	2.187.229,00	
	04	2.187.229,00	
	05	2.187.229,00	
	06	2.187.229,00	
	07	2.187.229,00	
	08	2.187.229,00	
	09	2.187.229,00	
	10	2.187.229,00	
	11	2.187.229,00	
	12	2.187.229,00	
2005			**26.246.748,00**
	01	2.187.229,00	
	02	2.187.229,00	
	03	2.187.229,00	
	04	2.187.229,00	
	05	2.187.229,00	
	06	2.187.229,00	
	07	2.187.229,00	
	08	2.187.229,00	
	09	2.187.229,00	
	10	2.187.229,00	
	11	2.187.229,00	
	12	2.187.229,00	
2006			**26.246.748,00**
	01	2.187.229,00	
	02	2.187.229,00	
	03	2.187.229,00	
	04	2.187.229,00	
	05	2.187.229,00	

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls: 1053
3685
Doc:

FINALIDADE
REDIR: Pregão 050/03 - Aluguel de servidores para expansão CCD - 48 meses

RESP. PELA EMISSAO

CHEFE/DORC
Delci Ribeiro da Costa
Coord/DEORC
Mat. 8.009.971-6

CHEFE/DEORC
Jameson Reinaux da Cunha
Chefe Depto de Orçamento e Custos
Mat. 8.011.115-7

	06	2.187.229,00
	07	2.187.229,00
	08	2.187.229,00
	09	2.187.229,00
	10	2.187.229,00
	11	2.187.229,00
	12	2.187.229,00
2007		21.872.290,00
	01	2.187.229,00
	02	2.187.229,00
	03	2.187.229,00
	04	2.187.229,00
	05	2.187.229,00
	06	2.187.229,00
	07	2.187.229,00
	08	2.187.229,00
	09	2.187.229,00
	10	2.187.229,00

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls: 1054
3685
Doc:

FINALIDADE

REDIR: Pregão 050/03 - Aluguel de servidores para expansão CCD - 48 meses

RESP. PELA EMISSAO

CHEFE/DORC
Delci Ribeiro da Costa
Coord/DEORC

CHEFE/DEORC
Jatreson Rureaux da Cunha
Chefe Depto de Orçamento e Custos

Hewlett Packard Brasil Ltda.
Alameda Rio Negro, 750 – Alphaville
06454-000 - Barueri - SP
CNPJ: 61.797.924/0001-55
Fone: (11) 4197 8000
Fax: (11) 4197 8432
www.hp.com.br

PROPOSTA ECONOMICA

PREGÃO Nº 050/2003 – CPL/AC

1. Hewlett-Packard Brasil Ltda
2. CNPJ nº 61.797.924/0001-55
3. I.Est. nº 206.203.572.117
4. Insc. Municipal.: 4-00.878-1
5. Al. Rio Negro, 750 – Alphaville – Barueri/SP – CEP.: 06454-000
6. Tel.: 11.4197.8000 - Fax.: 11.4197.8432 e-mail.http://voc.brazil.hp.com
7. Validade da Proposta: 60 (sessenta) dias
8. Prazo de Pagamento:
9. Banco: Itaú S/A Agência:0912 Conta Corrente:08067-8
10. Representante da Empresa: José Eduardo Pires do Rio Ribeiro e Denis Mineiro Santos
11. Representante de Vendas, RG 15.319.247(SSP/SP) e CPF 071.885.858-14 e RG. 2.004.658.809 E CPF nº 248.703.740-72.

Apresentamos nossa Proposta para locação de equipamentos de informática – novos de fábrica – incluindo instalação, configuração, treinamento e operação assistida do pessoal encarregado, assistência técnica, garantia e instalação dos PRODUTOS locados, do objeto do Pregão nº 050/2003, acatando todas as estipulações consignadas no Edital, conforme abaixo:

1. ASPECTOS FINANCEIROS

1.1. **O VALOR MENSAL DA LOCAÇÃO** para cada produto constante das condições especificas da contratação – **ANEXOS 1, 1-A e 1-B** – para o período de **48 (quarenta e oito) meses**, conforme tabela abaixo:

CORREIOS

CPL/AC RCT

MAPA COMPARATIVO DE PREÇOS

LICITAÇÃO: Pregão n.º 050/2003-CPL/AC

Data da Sessão: 24/07/2003

DESCRIÇÃO	EMPRESA/VALOR TOTAL DA LOCAÇÃO (*)				VALOR DE REFERÊNCIA (R$) **
	HP BRASIL	ITAUTEC	NEC DO BRASIL	COBRA	
Locação e instalação de 162 equipamentos de informática – novos de fábrica, incluindo: a configuração, o treinamento, a assistência técnica e a garantia	106.036.870,00	107.009.500,00	215.299.671,76	225.463.294,32	145.713.124,35

( )Valor da locação já incluso o valor de 1% do valor total da locação, relativo detalhamento do cronograma de trabalho.*
(**) Valor de referência fornecido pelo DECAM, com base na média dos valores da pesquisa de mercado.

Legenda :

Empresa Vencedora

CONDIÇÕES DE PAGAMENTO: 1% do valor total da locação, pago em parcela única, no 15º dia útil após a emissão do Termo de Aceitação da Fase I (Apresentação do cronograma) e 48 parcelas iguais, no 15º dia útil do mês subseqüente ao da prestação dos serviços, após a emissão do Termo de Aceitação da Fase III (Aceitação final dos equipamentos).
VALIDADE DA PROPOSTA: 60 dias, a contar da data de reunião de abertura da licitação.
PRAZO DE EXECUÇÃO DOS SERVIÇOS: 48 meses, a contar da data de emissão do Termo de Aceitação da Fase III (Aceitação final dos equipamentos).

Marta Maria Coelho
Pregoeira

Equipe de Apoio: **Gilberto Ferreira do Amaral**

Adriana Maria da Rocha Fonseca

Marise da Consolação C. Capella

Pedro Alberto da Silva Oliveira

CPLI - CORREIOS
Fls: 1056
Doc: 3685

E:\DIRAD\CPL\Documentos2003\Mapa Comparativo de Preços\Mapa Comparativo PG050_2003 Serviço locação servidor.doc

CORREIOS

Comissão Permanente de Licitação da Administração Central - CPL/AC

ATA DE REUNIÃO DE LICITAÇÃO
PREGÃO N.º 050/2003 - CPL/AC

OBJETO: Locação e instalação de 162 equipamentos de informática – novos de fábrica, incluindo: a configuração, o treinamento, assistência técnica e a garantia.

DIA/HORA: 24/07/2003 das 09:00 à 01:00 hora do dia 25/07/2003.

ASSUNTO: Esta Sessão destinou–se a abertura do Pregão n.º 050/2003-CPL/AC objetivando a obtenção da proposta mais vantajosa para a Administração, por meio de lances verbais disputados entre as licitantes. Foram recebidos e abertos os envelopes das propostas econômicas e o envelope de habilitação da firma vencedora.

LOCAL: Salão Nobre, localizado no SBN, Quadra 01, Bloco "A" - 1º sobreloja, do Ed. Sede da ECT, em Brasília/DF.

QUANTIDADE DE EDITAIS RETIRADOS: Foram retirados 79 (setenta e nove) exemplares do Edital, sendo 10 (dez) através do sistema impresso e 69 (sessenta e nove) através do sistema magnético, via Internet.

CREDENCIADOS: Compareceram à Sessão 04 (quatro) empresas relacionadas nesta ata.

ABERTURA DAS PROPOSTAS ECONÔMICAS: Após o credenciamento das participantes, procedeu-se a abertura e análise dos envelopes das propostas econômicas. Os preços unitários e totais cotados foram lidos para que os presentes tomassem conhecimento, conforme discriminado a seguir:

1-A) 21 SERVIDORES INTEL TIPO 01; **1-B)** 35 SERVIDORES INTEL TIPO 02; **1-C)** 51 SERVIDORES INTEL TIPO 03; **1-D)** 11 SERVIDORES RISC TIPO 01; **1-E)** 4 SWITCHES TIPO 01; **1-F)** 6 SWITCHES TIPO 02; **1G)** 6 SWITCHES TIPO 03; **1-H)** 12 SWITCHES TIPO 04; **1-I)** 2 SWITCHES TIPO 05; **1-J)** 2 ROTEADORES TIPO 01; **1-L)** 2 ROTEADORES TIPO 02; **1-M)** 2 UNIDADES DE BACKUP ROBOTIZADO; **1-N)** 4 SERVIDORES DE SEGURANÇA LÓGICA TIPO 01;**1-O)** 2 SERVIDORES DE SEGURANÇA LÓGICA TIPO 02; e **1-P)** 2 SERVIDORES PARA DETECÇÃO DE INTRUSÃO:

EMPRESA	DESCRIÇÃO DO ITEM	QTDE.	PREÇO UNITÁRIO MENSAL (R$)	TOTAL MENSAL (R$)
ITAUTEC INFORMÁTICA S/A	1-A – SERV. TIPO 01	21	43.529,83	914.126,43
	1-B- SERV. TIPO 02	35	10.094,75	353.316,25
	1-C- SERV. TIPO 03	51	6.200,12	316.206,12
	1-D – SERV. RISC 01	11	97.694,37	1.074.638,07
	1-E SWITCH TIPO 01	04	46.753,28	187.013,12
	1-F - SWITCH TIPO2	06	2.718,84	16.313,04
	1-G - SWITCH TIPO3	06	44.414,25	266.485,50
	1-H - SWITCH TIPO4	12	9.105,27	109.263,24
	1-I- SWITCH TIPO5	02	24.131,98	48.263,96
	1-J – ROT. TIPO 01	02	12.854,11	25.708,22
	1-K – ROT. TIPO 02	02	3.927,21	7.854,42
	1-L –UNID. BACKUP	02	158.038,73	316.077,46
	1-M- SERV. LOG. T-01	04	93.318,65	373.274,60
	1-N - SERV. LOG. T-02	02	13.789,88	27.579,76
	1-O – SERV. DETEC.	02	11.053,35	22.106,70

NEC DO BRASIL S/A	1-A – SERV. TIPO 01	21	23.326,86	489.864,06
	1-B- SERV. TIPO 02	35	11.632,43	407.135,05
	1-C- SERV. TIPO 03	51	2.891,10	147.446,10
	1-D – SERV. RISC 01	11	78.538,70	863.925,70
	1-E SWITCH TIPO 01	04	59.639,38	238.557,52
	1-F - SWITCH TIPO2	06	7.072,25	42.433,50
	1-G - SWITCH TIPO3	06	144.455,18	866.731,08
	1-H - SWITCH TIPO4	12	2.413,13	28.957,56
	1-I- SWITCH TIPO5	02	34.798,35	69.596,70
	1-J – ROT. TIPO 01	02	27.366,82	54.733,64
	1-K – ROT. TIPO 02	02	19.138,42	38.276,84
	1-L –UNID. BACKUP	02	431.962,84	863.925,68
	1-M- SERV. LOG. T-01	04	20.571,80	82.287,20
	1-N - SERV. LOG. T-02	02	23.558,04	47.116,08
	1-O – SERV. DETEC.	02	100.006,56	200.013,12
COBRA TECNOLOGIA S/A	1-A – SERV. TIPO 01	21	37.719,62	792.112,02
	1-B- SERV. TIPO 02	35	9.403,94	329.137,90
	1-C- SERV. TIPO 03	51	3.800,71	193.836,21
	1-D – SERV. RISC 01	11	136.006,10	1.496.067,10
	1-E SWITCH TIPO 01	04	130.189,25	520.757,00
	1-F - SWITCH TIPO2	06	3.517,50	21.105,00
	1-G - SWITCH TIPO3	06	45.107,38	270.644,28
	1-H - SWITCH TIPO4	12	49.726,75	596.721,00
	1-I- SWITCH TIPO5	02	4.387,50	8.775,00
	1-J – ROT. TIPO 01	02	22.684,50	45.369,00
	1-K – ROT. TIPO 02	02	4.768,00	9.536,00
	1-L –UNID. BACKUP	02	96.057,50	192.115,00
	1-M- SERV. LOG. T-01	04	28.485,25	113.941,00
	1-N - SERV. LOG. T-02	02	14.600,50	29.201,00
	1-O – SERV. DETEC.	02	15.664,00	31.328,00
HP BRASIL LTDA.	1-A – SERV. TIPO 01	21	18.831,24	395.456,04
	1-B- SERV. TIPO 02	35	4.272,08	149.522,80
	1-C- SERV. TIPO 03	51	2.881,23	146.942,73
	1-D – SERV. RISC 01	11	110.328,55	1.213.614,05
	1-E SWITCH TIPO 01	04	25.586,63	102.346,52
	1-F - SWITCH TIPO2	06	627,90	3.767,40
	1-G - SWITCH TIPO3	06	14.668,73	88.012,38
	1-H - SWITCH TIPO4	12	4.079,65	48.955,80
	1-I- SWITCH TIPO5	02	2.829,07	5.658,14
	1-J – ROT. TIPO 01	02	8.602,54	17.205,08
	1-K – ROT. TIPO 02	02	2.263,04	4.526,08
	1-L –UNID. BACKUP	02	161.976,95	323.953,90
	1-M- SERV. LOG. T-01	04	2.405,68	9.622,72
	1-N - SERV. LOG. T-02	02	2.405,68	4.811,36
	1-O – SERV. DETEC.	02	3.257,38	6.514,76

NOME DAS EMPRESAS	RODADAS DE LANCES				
	25ª	26ª	27ª	28ª	29ª
HP BRASIL	120.375.000,00	120.373.000,00	120.371.000,00	120.369.000,00	120.367.000,00
ITAUTEC	120.376.000.00	120.374.000,00	120.372.000,00	120.370.000,00	120.368.000,00

(*) Desistência de Lance

NOME DAS EMPRESAS	RODADAS DE LANCES				
	30ª	31ª	32ª	33ª	34ª
HP BRASIL	120.265.000,00	120.164.000,00	120.063.000,00	119.787.000,00	119.487.000,00
ITAUTEC	120.266.000,00	120.165.000,00	120.064.000,00	120.000.000,00	119.687.000,00

(*) Desistência de Lance

NOME DAS EMPRESAS	RODADAS DE LANCES				
	35ª	36ª	37ª	38ª	39ª
HP BRASIL	118.887.000,00	118.786.000,00	118.749.000,00	118.693.000,00	118.637.000,00
ITAUTEC	119.387.000,00	118.787.000,00	118.750.000,00	118.700.000,00	118.650.000,00

NOME DAS EMPRESAS	RODADAS DE LANCES				
	40ª	41ª	42ª	43ª	44ª
HP BRASIL	118.587.000,00	118.547.000,00	118.539.000,00	118.227.000,00	117.987.000,00
ITAUTEC	118.600.000,00	118.550.000,00	118.540.000,00	118.530.000,00	118.220.000,00

NOME DAS EMPRESAS	RODADAS DE LANCES				
	45ª	46ª	47ª	48ª	49ª
HP BRASIL	117.587.000,00	117.287.000,00	116.867.000,00	116.757.000,00	116.657.000,00
ITAUTEC	117.980.000,00	117.580.000,00	117.280.000,00	116.860.000,00	116.750.000,00

NOME DAS EMPRESAS	RODADAS DE LANCES				
	50ª	51ª	52ª	53ª	54ª
HP BRASIL	116.557.000,00	116.457.000,00	116.357.000,00	116.257.000,00	116.157.000,00
ITAUTEC	116.650.000,00	116.550.000,00	116.450.000,00	116.350.000,00	116.200.000,00

NOME DAS EMPRESAS	RODADAS DE LANCES				
	55ª	56ª	57ª	58ª	59ª
HP BRASIL	116.057.000,00	115.497.000,00	114.997.000,00	114.757.000,00	114.557.000,00
ITAUTEC	116.100.000,00	116.000.000,00	115.450.000,00	114.950.000,00	114.700.000,00

NOME DAS EMPRESAS	RODADAS DE LANCES				
	60ª	61ª	62ª	63ª	64ª
HP BRASIL	114.487.000,00	114.387.000,00	114.287.000,00	114.247.000,00	114.241.000,00
ITAUTEC	114.500.000,00	114.450.000,00	114.350.000,00	114.250.000,00	114.242.000,00

NOME DAS EMPRESAS	RODADAS DE LANCES				
	65ª	66ª	67ª	68ª	69ª
HP BRASIL	114.229.000,00	114.219.000,00	114.209.000,00	114.199.000,00	113.987.000,00
ITAUTEC	114.230.000,00	114.220.000,00	114.210.000,00	114.200.000,00	114.100.000,00

NOME DAS EMPRESAS	RODADAS DE LANCES				
	70ª	71ª	72ª	73ª	74ª
HP BRASIL	113.949.000,00	113.899.000,00	113.487.000,00	113.387.000,00	113.287.000,00
ITAUTEC	113.950.000,00	113.900.000,00	113.850.000,00	113.450.000,00	113.380.000,00

QUADRO RESUMO		
NOME DA EMPRESA	VALOR TOTAL MENSAL (R$)	VALOR GLOBAL (R$)
HP BRASIL	2.520.909,76	121.003.668,48
ITAUTEC	4.058.226,89	194.794.890,72
NEC DO BRASIL	4.440.999,83	213.167.991,84
COBRA	4.650.645,51	223.230.984,48

CLASSIFICAÇÃO DAS PROPOSTAS/RODADAS DE LANCES:

Todas as propostas foram analisadas tecnicamente pela equipe técnica especialmente designada para este fim. As dúvidas surgidas das propostas das empresas **HP BRASIL, ITAUTEC, NEC DO BRASIL e COBRA** foram sanadas através de diligências junto às empresas, conforme DECLARAÇÕES em anexo, que farão parte das propostas das mesmas.

Após análise das propostas, foram classificadas e autorizadas a dar lances de acordo a alínea "d.2 " do edital as empresas relacionadas no quadro abaixo, iniciando as rodadas de lances com a empresa NEC DO BRASIL e terminando com a empresa **HP BRASIL** vencedora do certame com o preço total de R$ R$ 106.036.870,00 (cento e seis milhões e trinta e seis mil e oitocentos e setenta reais), incluído o 1% relativo a apresentação do cronograma de trabalho.

NOME DAS EMPRESAS	# VALOR TOTAL DA LOCAÇÃO (R$)	RODADAS DE LANCES			
		1ª	2ª	3ª	4ª
HP BRASIL	121.003.668,48	120.989.000,00	120.987.000,00	120.985.000,00	120.983.000,00
ITAUTEC	194.794.890,72	120.990.000,00	120.988.000,00	120.986.000,00	120.984.000,00
NEC DO BRASIL	213.167.991,84	*	*	*	*

 # Valor total da locação excluído o 1%, relativo a apresentação do cronograma de trabalho
(*) Desistência de Lance

NOME DAS EMPRESAS	RODADAS DE LANCES				
	5ª	6ª	7ª	8ª	9ª
HP BRASIL	120.981.000,00	120.979.000,00	120.969.000,00	120.959.000,00	120.949.000,00
ITAUTEC	120.982.000,00	120.980.000,00	120.970.000,00	120.960.000,00	120.950.000,00

NOME DAS EMPRESAS	RODADAS DE LANCES				
	10ª	11	12ª	13ª	14ª
HP BRASIL	120.939.000,00	120.929.000,00	120.919.000,00	120.909.000,00	120.899.000,00
ITAUTEC	120.940.000,00	120.930.000,00	120.920.000,00	120.910.000,00	120.900.000,00

(*) Desistência de Lance

NOME DAS EMPRESAS	RODADAS DE LANCES				
	15ª	16ª	17ª	18ª	19ª
HP BRASIL	120.889.000,00	120.789.000,00	120.689.000,00	120.589.000,00	120.489.000,00
ITAUTEC	120.890.000,00	120.790.000,00	120.690.000,00	120.590.000,00	120.490.000,00

NOME DAS EMPRESAS	RODADAS DE LANCES				
	20ª	21ª	22ª	23ª	24ª
HP BRASIL	120.389.000,00	120.387.000,00	120.385.000,00	120.379.000,00	120.377.000,00
ITAUTEC	120.390.000,00	120.388.000,00	120.386.500,00	120.380.000,00	120.378.000,00

(*) Desistência de Lance

NOME DAS EMPRESAS	RODADAS DE LANCES				
	75ª	76ª	77ª	78ª	79ª
HP BRASIL	113.187.000,00	113.177.000,00	113.167.000,00	113.157.000,00	113.147,000,00
ITAUTEC	113.280.000,00	113.180.000,00	113.170.000,00	113.160.000,00	113.150.000,00

NOME DAS EMPRESAS	RODADAS DE LANCES				
	80ª	81ª	82ª	83ª	84ª
HP BRASIL	113.137.000,00	113.127.000,00	112.997.000,00	112.947.000,00	112.897.000,00
ITAUTEC	113.140.000,00	113.130.000,00	113.000.000,00	112.950.000,00	112.900.000,00

(*) Desistência de Lance

NOME DAS EMPRESAS	RODADAS DE LANCES				
	85ª	86ª	87ª	88ª	89ª
HP BRASIL	112.847.000,00	112.499.000,00	112.449.000,00	112.399.000,00	112.349.000,00
ITAUTEC	112.850.000,00	112.500.000,00	112.450.000,00	112.400.000,00	112.350.000,00

NOME DAS EMPRESAS	RODADAS DE LANCES				
	90ª	91ª	92ª	93ª	94ª
HP BRASIL	111.297.000,00	110.187.000,00	109.997.000,00	108.997.000,00	108.497.000,00
ITAUTEC	112.300.000,00	111.200.000,00	110.150.000,00	109.950.000,00	108.900.000,00

NOME DAS EMPRESAS	RODADAS DE LANCES				
	95ª	96ª	97ª	98ª	99ª
HP BRASIL	108.400.000,00	108.300.000,00	108.200.000,00	108.050.000,00	107.900.000,00
ITAUTEC	108.450.000,00	108.350.000,00	108.250.000,00	108.100.000,00	107.950.000,00

NOME DAS EMPRESAS	RODADAS DE LANCES				
	100ª	101ª	102ª	103ª	104ª
HP BRASIL	106.000.000,00	104.987.000,00			
ITAUTEC	107.500.000,00	105.950.000,00	*		

(*) Desistência de Lance

HABILITAÇÃO DA VENCEDORA: Após conferência da documentação da empresa **HEWLETT PACKARD BRASIL LTDA.** vencedora do Pregão, a mesma foi considerada habilitada. O envelope da empresa **ITAUTEC INFORMÁTICA S/A** ficará em poder da Pregoeira até a assinatura do Contrato. Os demais envelopes foram devolvidos a seus representantes presentes ao ato.

ADJUDICAÇÃO: A Pregoeira declarou vencedora a empresa **HEWLETT PACKARD BRASIL LTDA.**, CNPJ n.º 61.797.924/0001-55, com o preço global da locação pelo período de 48 (quarenta e oito) meses de R$ 104.987.000,00 (cento e quatro milhões e novecentos e oitenta e sete mil reais), perfazendo o valor total da proposta de R$ 106.036.870,00 (cento e seis milhões e trinta e seis mil e oitocentos e setenta reais), já incluso o valor de R$ 1.049.870,00 (um milhão e quarenta e nove mil e oitocentos e setenta reais), correspondente a 1% (um por cento) do valor total da locação, conforme previsto no Anexo 1-A, item 1.2. do Edital.

COMUNICADO: Fica acertado com o representante da empresa **HEWLETT PACKARD BRASIL LTDA.** que o mesmo deverá apresentar até o dia 28/07/2003 (segunda-feira) a proposta com os preços unitários ajustados de acordo com o último lance formulado.

RGSSF 05/2005 - CN - CPMI - CORREIOS
1061
Fls:
3685
Doc:

24719
Fls

ENCERRAMENTO DA REUNIÃO: Nada mais havendo a tratar foi dada como encerrada a reunião, lavrada a presente Ata, que após lida e achada conforme, vai assinada pela Pregoeira e sua equipe e pelos representantes credenciados presentes ao ato.

Marta Maria Coelho
Pregoeira

Equipe de Apoio Administrativo:

Marise da Consolação Cerqueira Capella

Pedro Alberto da Silva Oliveira

Jeanne Roriz Suaden

Gilberto Ferreira do Amaral

Liana Aparecida de Araújo

Adriana Maria da Rocha Fonseca

Equipe de Apoio Técnico:

Edilberto Nerry Petry

João Amaro Alves Pessanha

Hugo Viana

Roberto Stefan F. de Aguiar

Rogers Luis Cunha Pereira

Jefferson Colombo B. Xavier

Alexandre Pinto de Oliveira

Joseph Michel

Ruy Ney Muniz Barbosa

Daniel de Moreira Queiroga

Representantes credenciados e as respectivas Empresas:

Empresa: ITAUTEC INFORMÁTICA S/A
Nome Representante: Jorge Ítalo Dimatteu Telles
Fone: (61) 323-3031 Fax: (61) 226-1251

Empresa: NEC DO BRASIL S/A
Nome Representante: Vair Doiche
Fone: (11) 6462-6190 Fax.: (11) 6462-7053

Empresa: HEWLETT PACKARD BRASIL LTDA.
Nome Representante: José Eduardo Pires do Rio Ribeiro
Fone: (11) 4197-8000 Fax: (11) 4197-8432
9924-6565

Empresa: COBRA TECNOLOGIA S/A
Nome Representante: Antonio Alves Ferreira
Fone: (21) 2442-8800 Fax.: (21) 2442-8814

24.736

EMPRESA	DESCRIÇÃO DO ITEM	QTDE.	PREÇO UNITÁRIO MENSAL (R$)	TOTAL MENSAL (R$)	correção	valor locação	valor total
ITAUTEC INFORMÁTICA S/A	1-A – SERV. TIPO 01	21	43.529,83	914.126,35	914.126,43		
	1-B- SERV. TIPO 02	35	10.094,75	353.316,15	353.316,25		
	1-C- SERV. TIPO 03	51	6.200,12	316.206,07	316.206,12		
	1-D – SERV. RISC 01	11	97.694,37	1.074.638,07	1.074.638,07		
	1-E SWITCH TIPO 01	4	46.753,28	187.013,10	187.013,12		
	1-F - SWITCH TIPO2	6	2.718,84	16.313,07	16.313,04		
	1-G - SWITCH TIPO3	6	44.414,25	266.485,53	266.485,50		
	1-H - SWITCH TIPO4	12	9.105,27	109.263,26	109.263,24		
	1-I- SWITCH TIPO5	2	24.131,98	48.263,97	48.263,96		
	1-J – ROT. TIPO 01	2	12.854,11	25.708,23	25.708,22		
	1-K – ROT. TIPO 02	2	3.927,21	7.854,43	7.854,42		
	1-L –UNID. BACKUP	2	158.038,73	316.077,46	316.077,46		
	1-M- SERV. LOG. T-01	4	93.318,65	373.274,60	373.274,60		
	1-N - SERV. LOG. T-02	2	13.789,88	27.579,76	27.579,76		
	1-O – SERV. DETEC.	2	11.053,35	22.106,71	22.106,70		
					4.058.226,89	194.794.890,72	196.742.839,63
NEC DO BRASIL S/A	1-A – SERV. TIPO 01	21	23.326,86	489.864,06	489.864,06		
	1-B- SERV. TIPO 02	35	11.632,43	407.135,05	407.135,05		
	1-C- SERV. TIPO 03	51	2.891,10	147.446,10	147.446,10		
	1-D – SERV. RISC 01	11	78.538,70	863.925,70	863.925,70		
	1-E SWITCH TIPO 01	4	59.639,38	238.557,52	238.557,52		
	1-F - SWITCH TIPO2	6	7.072,25	42.433,50	42.433,50		
	1-G - SWITCH TIPO3	6	144.455,18	866.731,08	866.731,08		
	1-H - SWITCH TIPO4	12	2.413,13	28.957,56	28.957,56		
	1-I- SWITCH TIPO5	2	34.798,35	69.596,70	69.596,70		
	1-J – ROT. TIPO 01	2	27.366,82	54.733,64	54.733,64		
	1-K – ROT. TIPO 02	2	19.138,42	38.276,84	38.276,84		
	1-L –UNID. BACKUP	2	431.962,84	863.925,68	863.925,68		
	1-M- SERV. LOG. T-01	4	20.571,80	82.287,20	82.287,20		
	1-N - SERV. LOG. T-02	2	23.558,04	47.116,08	47.116,08		
	1-O – SERV. DETEC.	2	100.006,56	200.013,12	200.013,12		
					4.440.999,83	213.167.991,84	215.299.671,76
COBRA TECNOLOGIA S/A	1-A – SERV. TIPO 01	21	37.719,62	792.112,02	792.112,02		
	1-B- SERV. TIPO 02	35	9.403,94	329.137,90	329.137,90		
	1-C- SERV. TIPO 03	51	3.800,71	193.836,21	193.836,21		
	1-D – SERV. RISC 01	11	136.006,10	1.496.067,10	1.496.067,10		
	1-E SWITCH TIPO 01	4	130.189,25	520.757,00	520.757,00		
	1-F - SWITCH TIPO2	6	3.517,50	21.105,00	21.105,00		
	1-G - SWITCH TIPO3	6	45.107,38	270.644,28	270.644,28		
	1-H - SWITCH TIPO4	12	49.726,75	596.721,00	596.721,00		
	1-I- SWITCH TIPO5	2	4.387,50	8.775,00	8.775,00		
	1-J – ROT. TIPO 01	2	22.684,50	45.369,00	45.369,00		
	1-K – ROT. TIPO 02	2	4.768,00	9.536,00	9.536,00		
	1-L –UNID. BACKUP	2	96.057,50	192.115,00	192.115,00		
	1-M- SERV. LOG. T-01	4	28.485,25	113.941,00	113.941,00		
	1-N - SERV. LOG. T-02	2	14.600,50	29.201,00	29.201,00		
	1-O – SERV. DETEC.	2	15.664,00	31.328,00	31.328,00		
					4.650.645,51	223.230.984,48	225.463.294,32
HP BRASIL LTDA.	1-A – SERV. TIPO 01	21	18.831,24	395.456,05	395.456,04		
	1-B- SERV. TIPO 02	35	4.272,08	217.875,91	149.522,80		
	1-C- SERV. TIPO 03	51	2.881,23	146.942,90	146.942,73		
	1-D – SERV. RISC 01	11	110.328,55	1.213.614,04	1.213.614,05		
	1-E SWITCH TIPO 01	4	25.586,63	102.346,53	102.346,52		
	1-F - SWITCH TIPO2	6	627,9	3.767,39	3.767,40		
	1-G - SWITCH TIPO3	6	14.668,73	88.012,37	88.012,38		
	1-H - SWITCH TIPO4	12	4.079,65	48.955,77	48.955,80		
	1-I- SWITCH TIPO5	2	2.829,07	5.658,14	5.658,14		
	1-J – ROT. TIPO 01	2	8.602,54	17.205,07	17.205,08		
	1-K – ROT. TIPO 02	2	2.263,04	4.526,08	4.526,08		
	1-L –UNID. BACKUP	2	161.976,95	323.953,91	323.953,90		
	1-M- SERV. LOG. T-01	4	2.405,68	9.622,74	9.622,72		
	1-N - SERV. LOG. T-02	2	2.405,68	4.811,36	4.811,36		
	1-O – SERV. DETEC.	2	3.257,38	6.514,76	6.514,76		
					2.520.909,76	121.003.668,48	122.213.705,16

DOCUMENTOS DE HABILITAÇÃO DO VENCEDOR DA RODADA DE LANCES

ATA DE REUNIÃO DE ADJUDICAÇÃO DO PREGOEIRO